Key considerations when selecting a Managed Hosting provider

A Wanstor Guide for IT Professionals

wanstor

Contents

wanstor

Introduction

Many IT Managers describe '*managed hosting*' as a physical server with an operating system behind it. With a third party vendor managing appropriate hardware, licensing software, and patching security vulnerabilities. In short - managed compute.

However in recent years, managed hosting has expanded to represent a wide variety of infrastructure components as the advancement of management practices has evolved for IT vendors.

It now incorporates a broad range of infrastructure variables, going way beyond traditional managed servers to include managed storage arrays, web, middleware, databases and the management of business applications.

Today, IT service providers must work with customers IT environments to embrace unique challenges and requirements in building hosting ecosystems. While hosting ecosystems offer many benefits to a business or not for profit organisation, finding the right service provider can be a confusing process.

Based on our 15+ years of experience of providing managed hosting services for hundreds of customers, Wanstor have in many cases discovered that many prospective customers are unhappy with their existing managed hosting provider.

The main reasons are usually because the customer has been forced into signing up for and paying for hosting services they actually do not require or the managed hosting solution they have purchased does not enable their business in any way.

At Wanstor we always believe things can be improved, and this document aims to help IT Managers avoid common mistakes with regards to managed hosting services. Although each organisation's managed hosting needs are different, there are a number of common considerations that should be taken into account when choosing a managed hosting provider

Whether you are moving your IT infrastructure to a managed hosting provider for the first time or looking to switch to a new provider, finding the right partner to keep your operations running 24x7x365 is a critical piece of the IT operational puzzle.

Working with a managed hosting partner can provide the benefits of lowering operational and personnel costs, increasing reliability and performance and re-directing resources.

This document should help to guide IT professionals through some of the key considerations when conducting a managed hosting provider search.

How redundant is your data centre?

The redundancy of a data centre's critical systems is a major factor for guaranteeing uptime. At the heart of every data centre is power and in particular power management.

It is well known that data centres with the highest levels of redundancy provide at least two totally independent, parallel paths of power all the way from utility to racks. This is known as the Redundant Isolated Path Power Architecture (see figure 1 below).

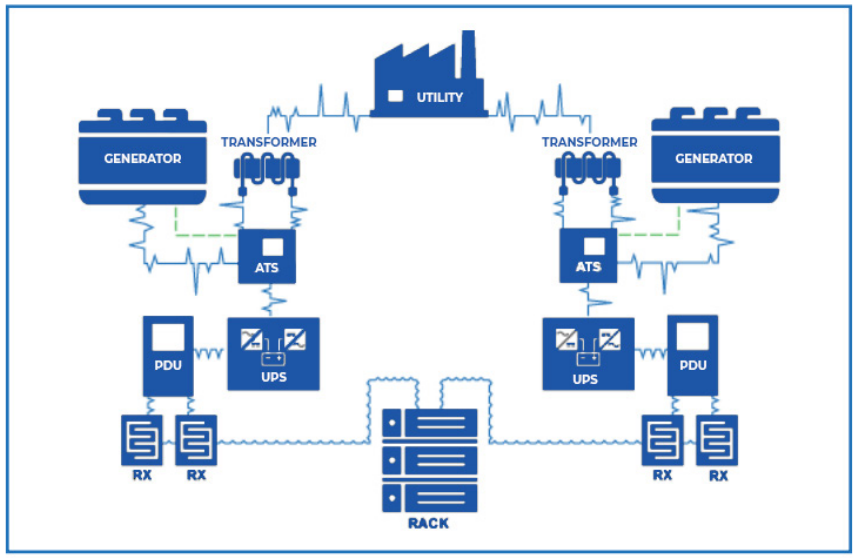


figure 1 : Redundant Isolated Path Power Architecture

A data centre with a Redundant Isolated Path Power Architecture maintains redundant sets of equipment that deliver reliable, protected and conditioned power along an isolated path from the utility to the data centre rack.

Each path has dedicated equipment including emergency power generation, independent fuel storage, uninterruptible power systems and power distribution systems, all of which remain isolated from equipment along other paths.

By using this model, if anything out of the ordinary happened, it would affect only one single path. Meaning the data centre could still operate.

However, most data centres electrical systems fall short of truly redundant power availability. Some data centres claim to operate in a redundant way, but are in fact using paralleling technology in their critical subsystems.

In a parallel system, the Uninterruptible Power Supply (UPS) and generators are connected together so that the load can be shifted back and forth, to equalize stress, in the event of a failure in a single device.

wanstor

The problem with this system is that it introduces complexity, which could ultimately harm the whole system.

Additionally, truly redundant data centres operate only Online UPS systems. meaning that the computers protected by the UPS are always powered directly by the UPS, which offers a more stable method of power conditioning and delivery.

A very redundant version of Online UPS system is a Double Conversion Online UPS system. A Double Conversion means that the utility power, which is Alternating Current (AC), is “rectified” into Direct Current (DC) and then is “inverted” back to AC power.

By going from AC to DC and back to AC, the power has been put through a double conversion. This double conversion means that the output power of the UPS system is completely clean, computer grade power that has been generated inside the data centre.

Many data centres run an “Offline” or “Line Interactive” UPS systems, which means that during normal operation, they really aren’t powering the computers connected to them. During normal operation, an Offline or Line Interactive UPS system only protects against extreme surges or failures of power.

Many distortions not in these extreme ranges, including damaging “Harmonics,” are allowed to get through to the computers. Data centre redundancy should also be built into the telecommunications infrastructure.

How secure is your potential managed hosting data centre?

At Wanstor we believe all managed hosting data centres should employ comprehensive security measures, from the physical characteristics of the building location all the way to the individual cameras located throughout the data rooms.

As a general set of rules, a managed hosting data centre should:

- Be constructed in a low traffic, nondescript setting which is easily accessible
- Be located in a geographically stable location with stable weather patterns, away from any environmental dangers such as floodplains, landslides and seismic faults. You should also look out for high winds, random acts of violence and other natural disasters that could have an impact on the facility
- All critical systems should be fenced off and monitored
- All entrances and externally located critical equipment should be alarmed, caged and surveilled by cameras that feed into the Network Operations Centre (NOC), which should be manned 24 x 7 x 365
- Access via critical doors should require dual factor authentication for entrance. All rooms and equipment inside the data centre should be monitored 24 x 7 by cameras that feed images to monitors in the NOC
- Recordings of monitoring images should be stored for 30 to 90 days and accessible on demand
- Each rack or cage should have individual locks, with keys maintained in a separate, lockable location accessible only by authorized data centre personnel
- Advanced systems should be in place to continuously report the status of the electrical and mechanical infrastructure to the NOC staff

The following is a suggested list of topics to ask your managed hosting data centre provider if, and how, they are monitored:

- Intrusion
- Fire
- AC power failure
- Generator failure
- Temperature & Humidity
- Breaker trips
- Leak Detection
- UPS failure

Data Centres that undergo compliance audits will have controls over information technology and related processes, policies and procedures, including operational activities that validate performance at optimal standards regarding security, availability and operating integrity.

A critical component of a truly secure facility is the creation of a culture that emphasizes and embodies the ideals of security.

When selecting a data centre partner, pay special attention to the measures taken by the data centre personnel to authenticate visitors to the facility by key card, biometric access systems or a combination of both.

Only authorized visitors should be granted access to their own, dedicated equipment in the facility after surrendering a government-issued ID to the onsite personnel. Phone based authentication is also critically important.

You need to feel safe that you are working with a partner who values your security and has built the systems and processes for ensuring it. External audits are one way to measure the ongoing effectiveness of a data centre's security policies and procedures.

All security systems should be monitored 24 x 7 and activities logged according to stringent controls and audited by a third party.

Certifications and audits

A data centre must have controls in place that comply with industry recognised standards. Standard audits and certifications for data centres include:

- PCI (payment card industry)
- GDPR and data protection rules by the ICO
- Logical and Physical Access
- Security of Environment and Information
- Backup & Recovery
- Secure Storage

The most common form of Industry Data is the Security Standard (PCI-DSS) is an information security standard for organisations that handle cardholder information for the major debit, credit, prepaid, ATM and POS cards.

The standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure.

Because data centres provide facilities for companies and merchants to house servers as they conduct their business, the data centre provider has specific responsibilities that must follow PCI compliance.

A merchant or company that is located within a PCI compliant data centre is not automatically PCI compliant.

Each merchant or company claiming PCI compliance must have and be able to provide their own confirmation of compliance, detailing their sensitive information procedures as they follow the PCI standard for example.

Connectivity

The connectivity of a managed hosting data centre is an important indicator of the reliability of its network and the flexibility you will have as a customer to find a network solution that works best for your business needs.

A data centre should provide bandwidth from multiple tier 1 providers

At the core layer, Border Gateway Protocol version 4 (BGP4) is the industry standard routing technology to automatically route traffic most optimally. By having multiple backbones and using BGP4 to decide how to send traffic to those backbones, the data centre is making Internet access much more reliable.

If either backbone or any router fails, the network automatically routes traffic around the interruption. During normal operation, the routing protocols make sure that packets are routed along the best path across the Internet on a route by route basis.

A well-connected data centre's network should be built on best-in-class, enterprise equipment, incorporating a core, an aggregation and an edge layer, deployed in a full mesh for the utmost redundancy.

The core of the network is comprised of a series of routers that connect directly to major Internet backbones. Each connection should be fibre-based Gigabit Ethernet lines, capable of transmitting 1 Gigabit per second (Gbps) or 1 billion bits per second.

The backbone connections should connect to their own backbone using SONET rings, which are miles long strands of fibre laid in a ring fashion so that if the fibre is cut in any place, traffic can automatically re-route around the other direction to the ring.

At the Edge layer, a data centre should be able to provide a twin drop to connect customers using Hot Standby Router Protocol (HSRP) and Gateway Load Balancing Protocol (GLBP) routing technologies to provide fault tolerance from the facility's networking equipment to the rack. A dual drop adds an additional layer of redundancy from the customer's rack to the Edge layer.

While most customers will use a "single" drop or a single wire to connect the Edge layer, those that cannot risk the possibility of an outage, due to a failed switch or router will request a dual drop. With a dual drop, the data centre adds another protocol or language into the customer connection to mediate the interaction of the two drops.

A well-connected data centre should also offer you options to connect directly, with the telecom provider of your choosing, for point to point or private connections.

Finally, it is important to make sure you have the flexibility to start small, with room to scale as you grow. Before you sign any contracts, make sure the data centre provider can accommodate the installation of additional equipment and networking capacity, on demand.

Does the data centre have the flexibility, in their contract terms, the design of their facility, and the responsiveness of their support group to accommodate that need quickly and effectively? How do they handle overage charges?

It is important to be working with a data centre partner that is truly flexible in their approach to supporting your connectivity needs as you scale and grow.

Support Levels

At Wanstor we have heard of managed hosting providers not providing 24/7 support. This means if your data requires access outside of business as usual hours you could be left stuck.

Wanstor therefore recommends that your data centre's Network Operations Centre is staffed 24/7/365 by on-site engineers that can actually provide hands-on help in the event of a problem or emergency.

Whilst you may think you will not require help for your *"rack"*, consider the benefits that an experienced network engineer can provide in the way of remote support when you need a server reboot or technical support above the hardware layer at 1AM.

While most data centre companies like to talk about support, they actually provide very little in the way of real, hands-on help.

A data centre that is strictly a *"ping, power and pipe"* facility may not even touch your equipment regardless of the situation. It is also important to ask for a definition of *"help"*.

Again at Wanstor, we have seen offers of *"help"* vary greatly between managed hosting providers.

Ask them to define their meaning of *"help"*. Do they provide server reboots or can they go deeper? Do they stop at the network layer or can they provide help all the way through layer 7, also known as the application layer, of the Open Systems Interconnection (OSI) Stack?

Who staffs their data centre after hours: a security guard or onsite engineers? Consider the travel time it will take for you or your team to make a special trip to your data centre in the event of an emergency.

Can you afford downtime in the event of a hardware failure? Ask your managed hosting provider how incident tickets are handled, how problems are escalated and what staff members are on-call both during and after business hours.

Is everything automated or do actual human beings answer the phones, respond to tickets and troubleshoot problems in your rack?

At Wanstor we are proud that our managed hosting data centres have 24/7 support by fully qualified engineers who our customers can actually come and meet in our central London office.

wanstor

Also, data centres that operate all the way through layer 7 of the OSI Stack provides several unique advantages, even if a customer doesn't foresee a need for support.

A data centre that is capable of application layer support will have the right experience in application development to diagnose, troubleshoot and remedy problems at the application layer.

In most cases, data centres that offer this level of support will have an onsite development team skilled at developing front and back-end application functionality giving them the distinct advantage of speaking the same language as their data centre customers.

They will have the necessary tools and resources onsite for their customers to be successful.

A data centre that is engaged with each layer of the OSI Stack can supplement a customer's capabilities, whether something is direct to their knowledge or they need immediate onsite support.

Disaster recovery and business continuity

A managed hosting partner should have the highest levels of security, redundancy, reliability and infrastructure necessary to house your servers. But it is also critical that your managed hosting partner has the right disaster recovery plan in place in order to support you remotely.

By definition your disaster recovery site will be located remotely from your business operations. It is important to make sure that your disaster recovery site has experienced personnel onsite to facilitate the installation, monitoring and maintenance of your equipment.

It is also important to make sure they can provide remote access for customers that are not able to travel and require immediate assistance to maintain online operations.

Additionally, if travel cannot be avoided, your disaster recovery site should provide dedicated workspaces, seats and conference rooms. A data centre partner for disaster recovery should also work with you to help identify your Recovery Time Objective (RTO) and Recovery Point Objective (RPO). RTO is the maximum length of time that a system can be down after a failure or disaster occurs before the company is negatively impacted by the downtime.

RPO specifies a point in time that data must be recovered and backed up. The RPO determines the minimum frequency and at which intervals backups need to occur, whether every hour or every five minutes.

Cloud-based disaster recovery is a good choice for organisations that need a secondary infrastructure where they can spin up resources on-demand or replicate their data in the event that they need to failover to the disaster recovery site in an emergency.

When the emergency is over, operations can failback to the primary site.

As referenced earlier, any information that resides in a cloud environment should be stored on dedicated equipment, devoted solely to the use of one customer. This private environment eliminates the security risks associated with operating in a shared cloud.

What kinds of tools and resources should be available to me as a customer?

Whether or not you plan on making regular trips to your managed hoisting data centre, it is best practice to find out what tools and resources the data centre makes available to customers and whether these tools are accessible and available for use 24/7/365.

Most data centres require customers to bring everything they need to work in their server cabinet or rack. But a true data centre partner should have many of these tools and resources on site.

Emergencies rarely happen during regular business hours. If you experience a hardware failure or server emergency at 2AM, consider the feasibility for you or your IT manager to drive to your data centre and troubleshoot the problem.

As a data centre customer, you are more likely to be successful choosing a data centre whose technical staff have deep experience at every layer of the OSI stack, regularly work on server and networking hardware and have the ability to assist you on demand.

A top tier facility that has an onsite, experienced technical support staff, will not only have a complete supply of tools, on-hand, for customer use.

They will also have staging areas, diagnostic equipment, office space and conference areas enabling you to host a meeting or just take a break. Moreover, the data centre should have spare servers, hardware and software available for customer use in the event of a failure or other emergency. Below is a checklist of resources that a data centre should have on-hand for customer use:

- Spare servers
- Spare firewalls
- Spare content switches
- Spare KVM switches
- Spare Ethernet wire
- Server lifts
- Spare cage nuts
- Standard tools
- Spare cable ties
- Cable testers

Understanding Pricing

Let's get down to the business of pricing.

Price is an obvious deciding factor in choosing a managed hosting provider. Unfortunately, price can be a misleading variable with hidden challenges. When comparing prices for managed hosting services, IT managers need to make sure that they are comparing like for like services. A key problem arises when comparing bundled services to à la carte services.

Some providers may offer lower prices by omitting features, so unless you check the service details, you may later discover that key features are omitted or are à la carte, increasing costs. Conversely, bundles might include services that you don't need, wasting money that would be better spent elsewhere. Take the time to understand exactly what each managed hosting provider will include for a given price

Consider all aspects of proposed services when making comparisons, requesting to know what specific services the provider delivers. For example, if you manage the data centre infrastructure, find out who will deliver the network. If you are migrating and optimizing infrastructure, determine whether you require a systems integrator.

It is crucial to work with a provider that enables you to leverage your core competencies while complementing your IT environment to build out the hosted ecosystem specific to your business or not for profit organisation.

Additionally, when comparing against keeping it in-house, it is essential that all costs associated with internal implementations are judged against using a provider's service. These include not just the cost of hardware, but any associated resources, including salary allocations, added power consumption costs, as well as costs associated with maintenance. All of these pricing considerations come down to knowing exactly what you need and comparing that to what a service provider offers. Price is important but it's not the only consideration.

Price Considerations

- *À-la-carte* or bundled
- Breadth of services offered
- Off-the-shelf or customized offerings
- Compare against all related internal costs from salaries to upkeep to maintenance

Understanding Contract Terms

Your contract determines who does what, when, and how. Understanding the specifics of a service contract can save IT Managers time and effort down the road.

At Wanstor we suggest you pay particular attention to the termination language. Often, your business needs change, and a provider's flexibility to change with you may be critical. Lastly, a service provider may not live up to the contract.

> **If you find that your service provider can no longer meet your requirements, regardless of the reason, consider finding a new provider**

Be careful, however, as you may find that terminating the service contract comes with severe penalties. Before signing a contract, check for amicable terms that will give you the flexibility to migrate between services without penalty.

Service-level agreements are also important, and critical in times of crisis, and need to be in the contract terms. Never assume that a service provider will meet particular SLAs, even if you have discussed them.

Make sure that the contract specifies the exact SLAs that you need.

Additionally, check to see if the SLAs are simply standard or if they have been customised to meet your needs. If you need SLAs tailored to your business, make sure that the contract spells out your exact requirements.

Finally, make sure that the contract is flexible. Do not be tempted to lock yourself into capabilities that you will not need in the future, but also do not lock yourself out of capabilities that you will need. The key word in contract negotiations is balance.

Ideally, IT Managers will want to balance locking down every detail with giving their company or not for profit organisation room to grow. Since no-one can predict future IT needs, flexibility in the contract is key to smooth IT operations.

Contract Considerations

- Amicable termination language
- Include exact SLAs needed
- Flexible terms

Understanding Strategic Issues

Strategic issues are broad concerns about how your company and your prospective service provider will operate together.
For example, geographical location could be a strategic issue.

In today's mindset of cloud services and global reach, it's easy to overlook the real issues that enterprises face with geography and data sovereignty. Co-location facilities, for example, should be neither too close nor too far away from your facilities.

If they are too close, then they are more likely to be affected by local disasters such as flooding. If they are too far away, they may suffer latency issues. Geographical concerns also affect the interactions of on-premise infrastructure and outsourced components causing potential latency issues.

Also, you may have infrastructure in a third-party data centre that needs to stay there. If so, make sure that your prospective service provider can work with it.

IT managers should also evaluate the technical capabilities of service providers. Their proposals should appear reasonable given their infrastructure. If a claim sounds too good to be true, it probably is.

Question absolute claims such as 100% uptime. Absolute claims sound good on paper, but the real world is not always possible. Measure claims against realistic expectations.

Corporate culture is another key strategic concern and one that is not always readily apparent. Two companies may both do excellent work - this does not mean that they can work together effectively.

Spend some time getting to know the culture of your prospective vendor to see if your company's way of doing business is compatible with how that service provider operates.

Strategic Considerations

- Geography
- Technical Competencies
- Corporate Culture

Understanding Performance

Another key area to consider when selecting a managed hosting partner is each service provider's performance as a company. One key aspect is longevity, how well established the service provider is in the industry. A provider with a long service history is likely to continue that performance in the future. Past performance doesn't always predict the future, but it is usually a good indicator.

More mature service providers with a 10+ year trading history are probably not going to go out of business suddenly, since they have had time to deal with growing pains. This is not to say, however, that newer service providers are unreliable. They will simply not have as much presence in the industry because they are new.

Newer providers may lack the stability of older companies, but they may be more innovative and flexible, and service providers' investments in technology and expertise are key indicators here. Newer providers need to differentiate themselves in the market, and they typically innovate via agile methodologies.

However, well-established service providers should be moving towards agile to answer the demands of the new application economy. Ideally, you would want a service provider with a long history of reliability, as well as a track record of innovation and staying at the cutting edge of technology and skill. To stay current, service providers will typically develop partnership communities, such as committing resources to support, developing specific opensource projects - determine what kind of community your prospective provider has, and how you can access it.

The road map for managed services is also vital. Managed hosting services don't appear overnight. Your chosen vendor needs to have a specific plan for delivering them, including guidelines for transitioning from your current model to the new services.

Finally, a good managed hosting service provider should avoid discussing only their own capabilities. They should focus on your objectives and requirements. Ideally, vendors should be asking you what you need.

Performance Considerations

- Provider Longevity
- Agile Methodologies
- Track Record
- Roadmap

Understanding the Support Model

Support is a tool, and like any tool, IT Managers need to understand how it works in order to use it effectively. At Wanstor, we suggest IT Managers check managed hosting providers across 3 core areas:

Support services

Some service providers offer 24/7 support, so you will be covered no matter when you need help. Others offer support only during business hours. If after-hours support is not much of a concern for you, make sure that you learn how the provider handles after-hours support tickets and always check providers' response times.

If you're dealing with time-sensitive issues, paying for round-the-clock support might not be enough if your provider doesn't respond quickly enough.

Be careful about relying on average response times. Ask for different response times for different incidents so you can gain a full picture of support services.

Finally, ask where the support services are delivered from. Central London support will of course cost more than offshore support in, for example, Vietnam - but in an emergency, you may need hands-on help and those people in London will be able to respond quicker than those in Vietnam.

Service flexibility

As your business grows and changes, your service needs will change. This means your service provider will need to adapt in response to your changing business and IT environment. Make sure that your chosen provider can bring alternative platforms as required.

Also, while you may start out with a traditional managed hosting model, you should be able to move to a cloud-based model when needed.

You may find that you need a private, public, or hybrid environment in the future, so your service provider should have expertise in all of these areas even if you don't currently need them.

These issues demonstrate the need for strategic planning. You will not be able to anticipate every need, but you should be able to identify most of the major potential issues that your business will face in the future.

Security and governance

While security and governance are obviously vital issues for certain highly regulated industries like healthcare and finance, every company has confidential information to protect, from customer records to financial reports.

When you trust that information to a service provider, you need to be confident in the provider's security practices. Find out how potential service providers encrypt data at rest and in transit.

Compare those practices to industry standards. Your data should also be safe during a disaster, which means that you have two more considerations.

Firstly, offsite backup is a necessity for disaster recovery. Secondly, merely keeping data offsite is not enough. Business moves quickly, and so does your data. You need to know your service provider's backup strategy: how data is backed up and what data is included.

Understand their deduplication method, especially if you need to backup large amounts of data. Analyse how the data is stored and whether it is secure enough for your needs.

Also consider how the service provider handles restoring data. The provider's recovery time objective (RTO) and recovery point objective (RPO) need to be sufficient for your operations.

But make sure that the audits are meaningful and not just cursory checks. Service providers should follow industry standards for security audits, and they should have the appropriate certifications for their respective markets.

As always, make sure that your chosen provider meets your needs.

Support Considerations

- Hours of operation
- Guaranteed response time
- Onshore vs. offshore
- Service flexibility
- Security and governance
- Backup locations and strategy
- Security audits

Wanstor Cloud Hosting with true network integration

Wanstor's hosting platform provides IT Managers with greater freedom and security when configuring applications in the cloud. MPLS network integration allows you to migrate applications to a Wanstor UK data centre, but still integrate those applications with existing services and networking.

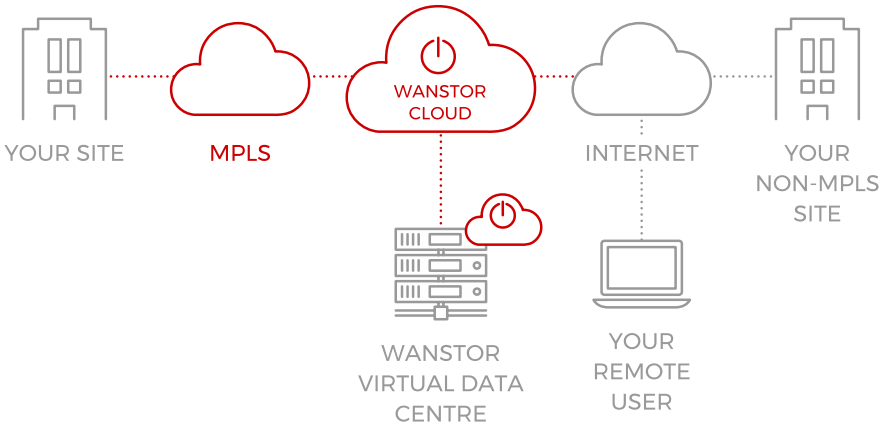
Strategy	Design	Integration	Procurement	Implementation	In-Life Management	Ongoing Maintenance
Cloud Service Model Definition	Cloud Technology Selection	Cloud Service Management Blueprints	Multi-Channel Sourcing	Logistics	Managed Infrastructure Service	Maintenance and Training Services
Cloud Sourcing Strategy	Cloud Implementation Blueprints	O365 Integration		Staging and Configuration	Managed Hybrid Cloud	
Maturity and Readiness Check		O365 Migration			Managed O365 Service	
O365 Readiness Check		Hybrid Cloud Migration Services				
		Public Cloud Integration				

wanstor

Wanstor's Private Cloud solutions to customers

The main private cloud solutions Wanstor provide to customers include:

How it works:



wanstor

Wanstor Managed Hosting Benefits

Lower IT costs

Matching your IT cost patterns to your computing demands. This means you can move IT from a capital-intensive cost model to an Opex model.

Cope with increased user demand

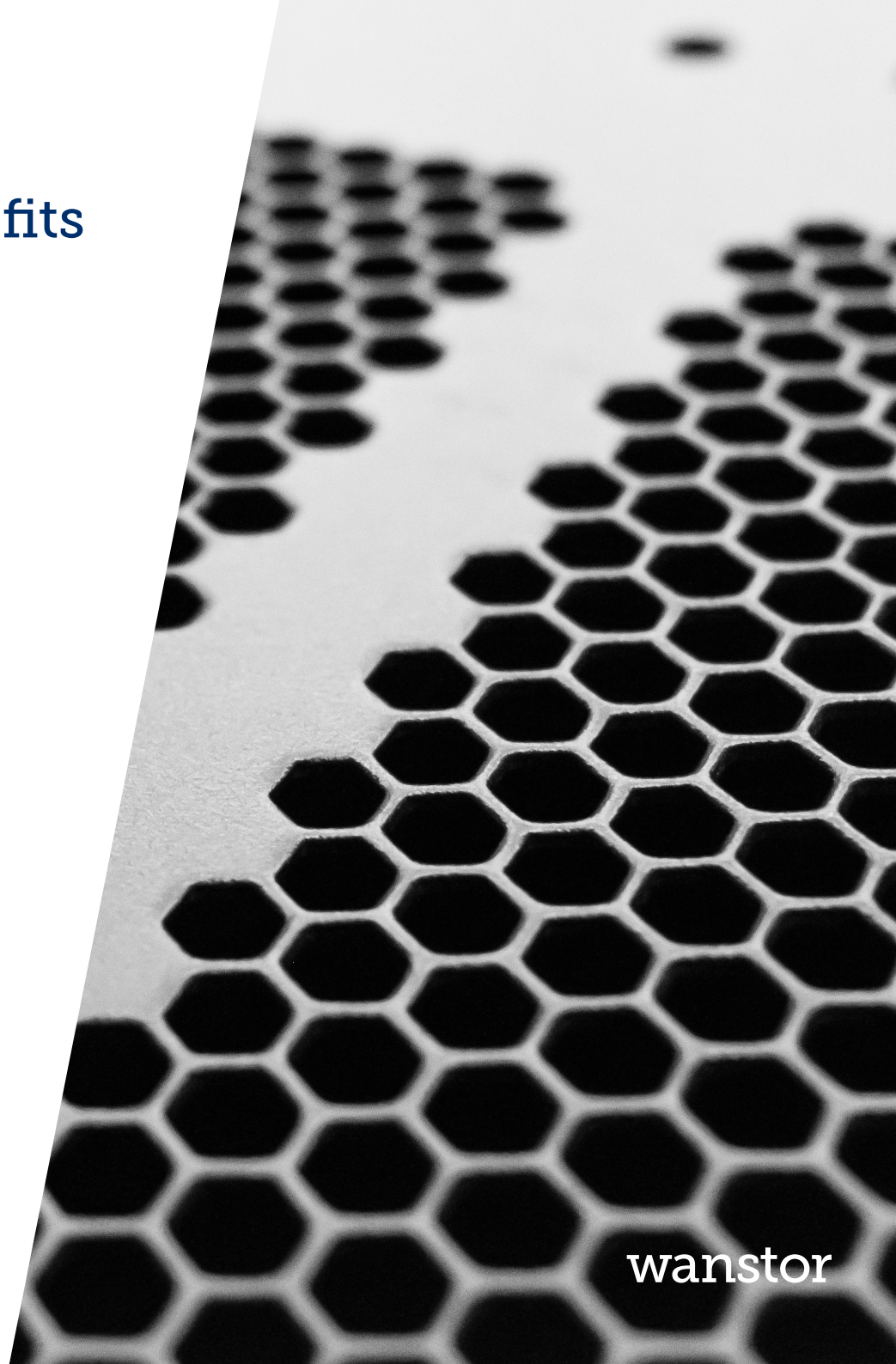
As your business grows, a cloud environment should grow with you. Managed hosting can also help your business when demand for IT is unpredictable or you need to test a new applications, giving the IT department control over capacity and paying only for what is used.

Run your business; don't worry about your IT

A managed cloud solution by Wanstor means we are doing this for you. In addition to monitoring your infrastructure and keeping your data safe, we can provide creative and practical IT solutions matched to your organisations needs.

Reduce your carbon footprint

Hosting in a cloud data centre rather than onsite allows you to take advantage of energy efficient technologies provided by your cloud partner.



Innovate and lead

Ever-changing business requirements mean that your IT infrastructure has to be flexible. With a cloud infrastructure, you can rapidly deploy new projects and take them live quickly, keeping you at the forefront of innovation.

Improved security and compliance

A managed private cloud environment provided by Wanstor means security and compliance is no longer just the IT team's responsibility, it is a joint one.

At Wanstor, we build in resiliency and agility into all cloud solutions at an infrastructure-level. This limits exposure to security breaches, and can help to improve your compliance and regulatory requirements.

Future-proof your business

There is unprecedented demand for access to data anywhere, any time and on any device. Don't let your business fall behind. By embracing the cloud, you can handle emerging mobile, digital and data management trends.

Why Wanstor?

- Recognised as a leader in managed hosting solutions
- UK support 24 x 7 x 365 for your critical infrastructure hosted on our premises
- Wide range of hosting services and management options
- Holistic service experience: hosting and networks
- UK accountability and ease of migration give you real control
- Self-service IaaS portal experience
- Wanstor manage the platform up to the hypervisor
- Library of virtual machine templates included public cloud, private cloud or hybrid cloud solutions
- Flexible *pay as you use* billing
- PCI DSS certified services
- Single portal view across your services

wanstor

Final Thoughts

Before you sign any contract you should evaluate a service provider carefully, based on the key considerations which have been described in this document.

Outline exactly what you receive for the price, and make sure that you have what you need without paying for extra services you do not require now or in the future.

Understand the contract terms by making sure that they don't lock you into that one provider, check that the SLAs are explicitly stated and tailored to your needs, and leave room for future requirements. Neither lock yourself into nor out of future capabilities.

Consider the strategic issues facing service providers, and examine the actual geographical locations of data centres to make sure that they fit your requirements without interference.

Take the time to evaluate the service provider's technical capabilities and corporate mentality as well, making sure that they are compatible with your business. Evaluate the service provider's performance, including the company's longevity, track record, workload support, and service road map.

Finally, learn the overall support model, and determine whether it's the right fit for your company in terms of support, service flexibility, and security.

With these considerations covered, IT Managers should be able to select the managed hosting provider that is right for their business.

For more information about Wanstor's managed hosting solutions please contact us on **0333 123 0360**, email us at **info@wanstor.com** or visit us at **www.wanstor.com**.