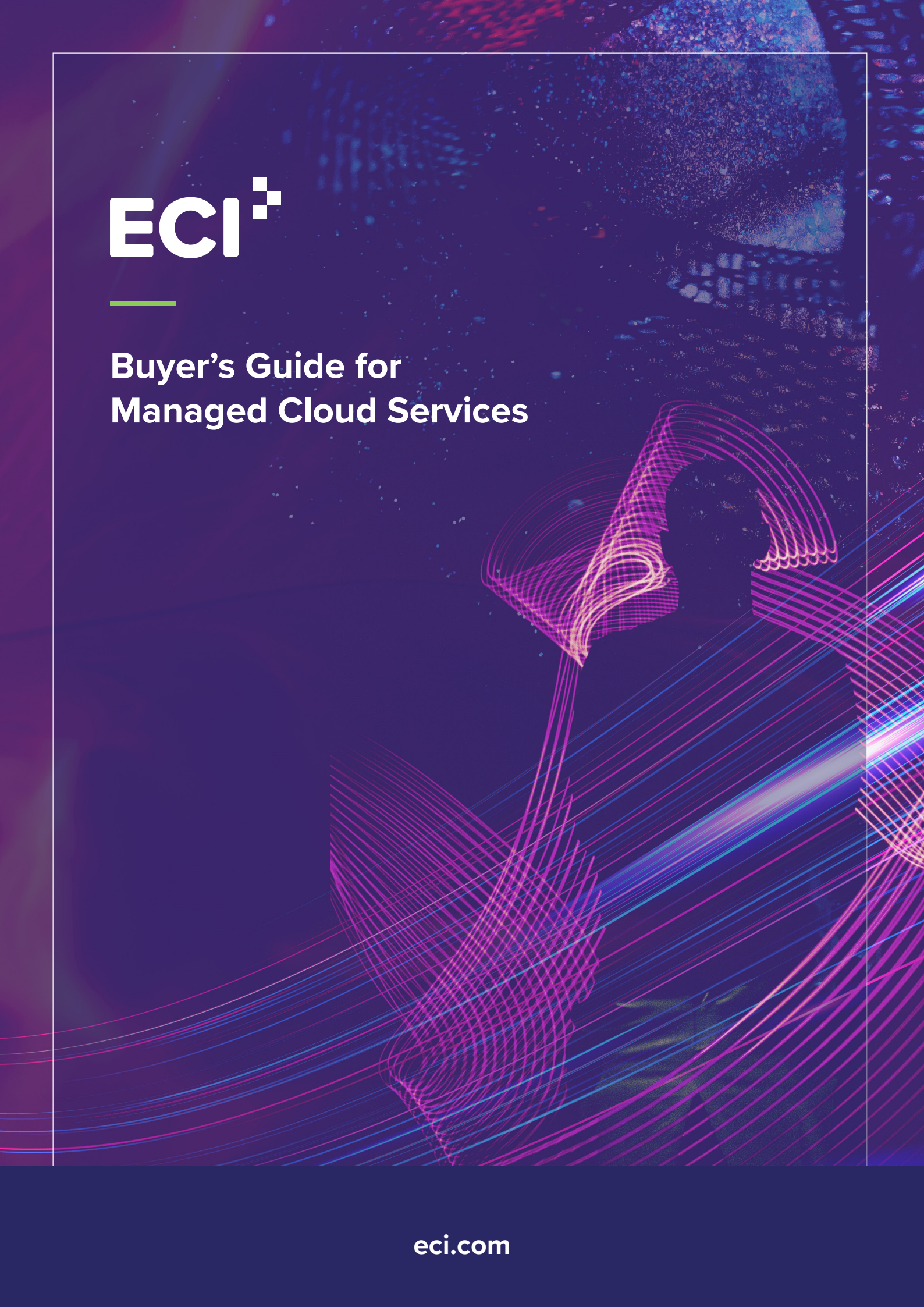


Buyer's Guide for Managed Cloud Services

eci.com

Contents

Part 1

Cloud Technology Evolves

Enterprise cloud computing technology has achieved industry standard status. Today, 94% of organizations worldwide use public or private cloud networks, or leverage platform-as-a-service, infrastructure-as-a-service, or software-as-a-service solutions. Meanwhile, more than 60% of corporate data is stored in the cloud.[1]

Of these cloud environments, an estimated 90% of enterprise cloud users maintain multi-cloud environments, meaning they have multiple disparate cloud solutions in place[2]. The widespread growth of the cloud-first approach and the growing popularity of hybrid/multi-cloud strategies (according to a Microsoft poll, 95% of IT pros said these environments are "critical to success"[3]) – will cause complications for businesses that are already stretching their IT teams thin.

Managed Cloud Solutions are key to overcoming this developing problem, as they enable organizations of all sizes to cultivate and utilize a robust cloud infrastructure, all without overburdening internal IT personnel. But what should you look for when sourcing such services? This buyer's guide will help you understand what to look for in a managed cloud services provider.

---

[1] Statista (https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data/)
[2] Statista (https://www.statista.com/statistics/1245569/multi-cloud-adoption-organization-size-worldwide/)
[3] Microsoft Hybrid and Multi-Cloud Perceptions Survey (https://blogs.microsoft.com/wp-content/uploads/prod/2022/01/Microsoft-Cloud-Survey-Results-Final.pdf)

Part 2

Cloud-first Approach

First thing's first. When evaluating managed cloud providers, it's critical to first evaluate your cloud methodology and recognize the role cloud technology will play within your overall IT strategy. Now that remote and hybrid work is a default, managing the challenges of this new model can impact your choice of managed cloud provider.

Consider the four inflection points that trigger the need for a managed cloud provider:

Security and availability. How do your employees access data across your expanding digital environment? Remote and hybrid work must be supported by a secure, highly available, zero-trust infrastructure.

Changing office landscape. Is your organization reducing your corporate office footprint to align with the needs of hybrid work schedules? Reimagining the office is a natural time to look at your existing technology infrastructure.

Emerging organization. Emerging organizations must think cloud-first. But before choosing a cloud model, they must also take budgetary or resource considerations into account and be cognizant of the future technology requirements of the business.

Technology refresh. Is your technology stack and IT strategy due for a refresh? The rush to remote/hybrid work has sped up digital transformation by several years putting pressure on IT departments to support new ways of working. This is a good time to evaluate automation and modern digital technologies so that IT teams can focus on the core business.

You'll need to a look at your IT priorities to decipher which cloud model is the best fit for your firm: public, private, hybrid or multi-cloud. A knowledgeable managed cloud provider will act as a consultant and partner when your organization is defining your overall cloud strategy. Look for a provider that has a cloud-agnostic approach, meaning they're able to support you and your IT initiatives regardless of which model is the best fit for your firm. Utilizing an experienced cloud services provider enables you to take full advantage of the cloud.

Part 3

Strong & Flexible Cloud Architecture

The underlying architecture governing how the cloud is designed and configured has an out-sized influence on data workflows and subsequent management and security requirements.

Depending on your goals, regulatory environment, and comfort-level, you can choose between public (e.g., Microsoft Azure) and private platforms (e.g., Azure Stack) both of which can be customized and managed so that you get more value for the cloud.

Look for a provider that can:

Offer **robust network and data center solutions** to ensure 24/7/365 availability and resiliency.

Integrate and streamline operations across multi-cloud environments.

Run and **manage workloads in geographically dispersed** regions for faster data delivery and an optimized user experience.

Ease the burden of **regulatory compliance and reporting.**

Give you **options and open lines of communications** for overseeing the configuration.

While you can't control the architecture behind your cloud, you can work with a provider that provides visibility and creates trust in managing your cloud ecosystem.

What to ask your cloud provider

How do you engage with me to **align our cloud strategy** with the needs of our business?
Do you have **direct connectivity** to public and private cloud platforms?
Where is my data stored and how do you handle **backup and recovery?**
How do you implement **zero-trust?**
What is your cybersecurity **incident response plan?**
What are my **responsibilities** in managing the configuration?
If my firm wants some control, is there a **self-service portal?**
What is the **response time** of your service organization?

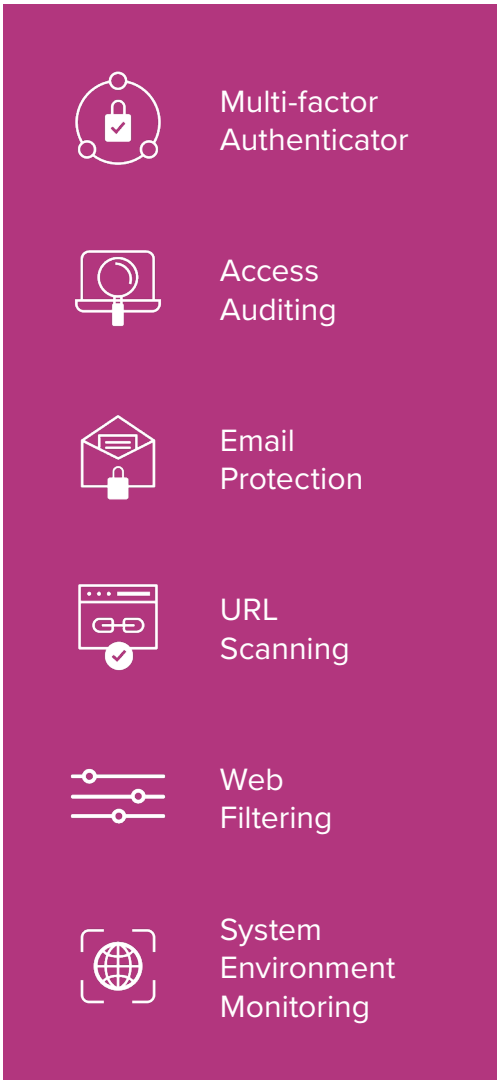
Part 4

Robust Cybersecurity Services

Data breaches are skyrocketing. In the past year, breaches stemming from cyberattacks jumped 68% to the highest total ever.[4] Meanwhile, ransomware attacks increased by 13%, a jump greater than the past five years combined.[5]

Don't let your business be next because your cloud provider has fallen behind on security or you've assumed that public cloud security controls are automatically activated. Instead, ensure your cloud provider:

- Complies with regulatory standards that apply to your business (HIPAA, PCI DSS, GDPR, new SEC cybersecurity rules, etc.) or major industry-wide regulations for data center reliability (SOC, Uptime Institute, ANSI/TIA).
- Takes a security-first approach to operations that prioritizes data protection when managing the cloud configuration.
- Provides physical and logical access control to protect against hackers, bots and similar threats.
- Uses modern security tools to protect the configuration:



[4] Identity Theft Resource Center 2021 Data Breach Report (https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/)
[5] Verizon DBIR 2022 (https://www.verizon.com/about/news/ransomware-threat-rises-verizon-2022-data-breach-investigations-report)

What to ask your cloud provider

Have you experienced a **security breach?**
What **security framework** does your firm follow?
Do you undergo a **SOC Audit** and regular **vulnerability assessments?**
What is your **incident response plan?**
If I suspect my organization is compromised, **who do I contact** and what is the response time?
What do we need to do to **protect the cloud on our end?**
What is being done to protect against **ransomware, dark web threats** and other **common attack types?**

Part 5

Reliable Backup Capabilities

IT pros understand the importance of proper backup and recovery strategies. However, the resources they use to manage data effectively aren't always given the same level of thought. As such, approximately 67% of IT pros believe the backup solutions at their current business are not capable of safeguarding data in the event of downtime or destructive cyberattack.[6]

Cloud computing can be a powerful tool in simplifying backup and recovery, but only if your cloud provider has adequate protections in place.

Not all managed cloud providers offer equally robust backup and recovery options. Be sure to carefully analyze your service level agreements to protect data and ensure you work with cloud providers that maintain off-site backup options that are available in real-time. Additionally, consider keeping your backups outside of your primary cloud provider - for example, if Microsoft cloud is your primary, maintaining additional backups in a non-Microsoft cloud helps remove single points of failure.

---

[6] Dell Technologies 2021 Global Data Protection Index (https://www.dell.com/en-us/dt/data-protection/gdpi/index.htm#pdf-overlay=//www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/global-data-protection-index-infographic-global.pdf)

What to ask your cloud provider

Do you practice recovering in emergency situations? If so, what is your **average recovery time?**
Do you maintain copies of our data in **multiple clouds** to reduce risk of downtime?
How do you safeguard backups from **ransomware** and **other cyber threats?**
How frequently do you back systems up?
Do you offer the ability to **run a secondary configuration** in duplicate with automated failover in place?

Part 6

Premier Customer Support

Managed cloud providers facilitate a variety of functions for their customers. They will often handle a wide range of critical systems, provide security, support, and similar services to empower businesses to take full advantage of the cloud.

With so much on the shoulders of your cloud provider, you don't want to be in a situation where you must jump through hoops to get support. When something isn't working, your team needs easy, efficient access to support from the managed cloud provider. Ask for a sample of their service level agreement (SLA) to see exactly what the provider guarantees in terms of service and support. Also, be sure to speak with their clients – large and small.

This 24/7/365 level of service is especially necessary in the multi-cloud world, where your IT department often serves as the go-between for support requests involving cloud providers. Don't make life difficult for your IT team. Instead, identify managed services providers that prioritize customer support and make it easy for your teams to get help.

Part 7

Streamlined Implementation Options & Migration Services

In the cloud-first world, departments often spin up a new service or environment for development purposes without aligning it to existing infrastructure or validating their approach.

Getting implementation right is key as the cloud becomes the de facto option for businesses. In 2022, the market for cloud services will **surge nearly 8% annually** as most large organizations are predicted to use external consultants to develop their cloud strategy.[7]

Make sure you ask questions about the rollout process during sales calls and see if you can get client referrals so you can learn more about what it's like to deploy a new solution with the managed cloud providers you're considering. You should also look for self-service tools and automation options to make it easier for you to make minor changes to the configuration.

Better yet – a top-shelf provider will streamline the implementation and perform migration services on your behalf, freeing time for your IT team to devote to other projects. This enables you to rely on your partner's expertise and can often expedite the implementation.

---

[7] Gartner (https://www.gartner.com/en/newsroom/press-releases/2022-01-18-gartner-forecasts-worldwide-it-spending-to-grow-five-point-1-percent-in-2022)

What to ask your cloud provider

What **pain points** do clients typically face during migration?
How will the migration impact **existing users?**
Are applications/tools (i.e., multi-factor authentication, spam filtering, etc) **changing?**
How will you **monitor, manage and patch applications** in the new environment?
What is your experience in **migrating firms to new cloud infrastructures?**
How long will the migration take from plan to go-live?

Part 8

Placing a Value on Cloud Connectivity

Whether a cloud is public or private, in today's hybrid world there are a variety of forces and interconnections at work behind every action an application or user makes. That's why understanding the connectivity of a cloud service should be included in the evaluation and purchasing process.

A key concept is a highly available, secure, and agile global network. A powerful cloud network infrastructure that connects multiple points of presence (data centers) around the world will ensure fast and scalable performance for all your apps and services – wherever they are deployed.

Whatever method you use to access the cloud – via the internet or a private connection – make sure the connection between your users and the cloud is secure, isolated, and private.

Part 9

Embracing the Cloud Computing Future

As cloud technology has matured, the volume of workloads running in the cloud continues to grow. Businesses aren't just dealing with a few apps and services in third-party configurations. Instead, the cloud increasingly handles mission-critical services and is so prevalent that most companies have multiple cloud environments to manage.

A modern cloud strategy requires solutions to help manage and secure your systems. Managed cloud services provide an edge, giving you access to development, support, and configuration management resources that you wouldn't get by simply moving to the cloud.

We are headquartered in Boston and have offices across the United States, Europe and Asia.

Contact us today to learn how we can help you on your cloud journey.

Corporate Headquarters:
55 Court St. Suite 520
Boston, MA 02108

Global Sales:
US | +1 800 752 1382
UK | +44 207 071 6802
Singapore | +65 6622 2345
Hong Kong | +852 3189 0101

For more information, visit:

eci.com