On-Premise Vs Cloud Software

The 6 Step Executive Guide

smarty

For businesses, the ability to move information quickly, correctly, and efficiently requires reliable software tools that can manage a huge amount of data that's being accessed and manipulated by multiple users, possibly in multiple locations. In addition to working with that information, companies are now responsible for keeping the data secure and disposing of it properly afterwards.

When it comes to managing their data, businesses need software that's:

- Quickly and easily deployed
- Able to be accessed and manipulated by multiple users
- Secure and reliable
- Compliant with their industry regulations
- Cost-effective for their needs

The right software will enable companies to keep their information safe and workflows running smoothly. One of the biggest questions in IT infrastructure planning is whether to go with on-premise or cloud software solutions. This question applies to many types of business software, including Customer Relation Management (CRM), Enterprise Resource Planning (ERP), Business Intelligence (BI), Geocoding, Address Validation, and more.

To decide which solution is right for your organization, you need to consider the following 6 factors:

1. Deployment Speed & Complexity
2. Control & Agility
3. Security, Reliability, & Uptime
4. Compliance
5. Total Cost of Ownership
6. Hybrid

This Executive Guide will shed light on each of these factors to help you make the best decision for your organization.

Cloud Computing Versus Cloud Services

You might see these terms used interchangeably, however they're not quite the same. A cloud system, or cloud computing technology, consists of hardware, software, and infrastructure that enables the delivery of cloud computing services (SaaS, PaaS, IaaS). Those services could be any of a wide range of services delivered on-demand to companies and customers over the internet.

01

ON-PREMISE VS CLOUD

Deployment Speed & Complexity

01 ON-PREMISE VS CLOUD DEPLOYMENT SPEED & COMPLEXITY

Your timeline and your data needs can help you make the decision of cloud computing vs on-premise technology. Do you need to implement your solution immediately, or can you spend some extra time customizing and configuring an on-premise solution?

On-Premise Deployment Speed & Complexity

With on-premise software, your company takes responsibility for maintaining the solution and related processes. The deployment is done in-house using your company's tech. On-premise implementations typically take longer due to the time needed to complete installations on servers and any individual computers or laptops.

While it requires more man hours and more staff, on-premise deployment gives you complete control. Your data, hardware, and software platforms are all yours. You decide on the configuration, the upgrades, and system changes. You can make your system as complex or as simple as you need. Companies with strong IT departments can create incredibly customized processes and workflows.

Cloud Deployment Speed & Complexity

With a cloud-based solution, the service provider maintains the systems on their server, accessible by your enterprise at any given time. A cloud-based solution is deployed over the internet in a matter of hours or days because nothing needs to be installed on a physical server or computers. Furthermore, maintenance and related processes are taken care of by the host-cloud service provider.

While the deployment is easier, cloud software is typically not as customizable as an on-premise solution. Depending on how it's hosted, a cloud solution may not be able to cope with complex development.

02

ON-PREMISE VS CLOUD

Control & Agility

"Agile" has become a big business buzzword these days, with organizations promoting their "agile leadership" and "agile management" or "agile development." But what is Agile, really?

Agile is a mindset represented by 4 values and 12 principles and manifested through various practices.

The concept started as an iterative and collaborative approach to software development and has flowed into many other areas of business.

It's been over 20 years since the creation of the Manifesto for Agile Software Development, and according to these 2022 Agile Adoption Statistics, 71% of companies have adopted Agile—even for non-IT functions.

Since the coronavirus pandemic swept the globe in early 2020, organizations are keenly aware of the opportunities and challenges ahead and realize being successful in the digital age requires agility in software development and delivery, as well as business strategy and operational execution. Being able to pivot quickly to changing market conditions, as well as customer and stakeholder demands, can mean the difference between success and failure.

However, achieving agility in your business's actions and reactions means more than just following the most well-known Agile practices. It requires a culture of continuous improvement.

Agility is the state of being Agile, not just doing Agile.

True agility recognizes that a company is a network of complex systems, and when you alter one, it impacts another, and you want all those systems to be moving together in the right direction. Which begs the question, will on-premise or cloud software aid you more in your quest for agility? And which is more important to your business needs: control or agility?

On-Premise Control & Agility

On-premise applications allow enterprises to maintain a level of control that the cloud often cannot. You have complete control and full access to your system locally. However, control comes at the cost of agility.

The time to install a system on premise takes considerably longer than a cloud solution would. In addition, scaling your on-premise infrastructure up or down would require additional time and expense. You might even require entirely new machines depending on how much you wanted to scale up. Anytime you make changes to an on-premise system, you sacrifice efficiency. In addition, you're committing a lot of IT hours to continuous internal upkeep of the hardware, software, data backups, storage, and disaster recovery.

Cloud Control & Agility

While you won’t have access to the physical servers, cloud services, and the cloud computing behind them, provide many benefits that can benefit your organizational agility, including scalability and flexibility, on-demand infrastructure, and automation.

SCALABILITY & FLEXIBILITY

The pay-per-use structure of most cloud service providers allows organizations the flexibility to scale up or down as their business needs change—without purchasing additional IT equipment or ending up with unused equipment gathering dust somewhere. Some common instances that require on-demand scalability: testing and development, load testing, seasonal spikes in traffic, or a new application.

ON-DEMAND INFRASTRUCTURE

While a physical server could take days or weeks to procure and set up, a cloud server takes minutes. The quicker a business can get its systems up and running, the quicker it can start earning revenue.

AUTOMATION

Cloud computing relies on distributing workloads and sharing resources to achieve coherence and economies of scale. It simplifies provisioning, de-provisioning and re-deploying resources through automation, APIs, and web consoles. Compared to an on-premise solution, a cloud system is much easier for an IT systems administrator to manage and support.

As always, there’s a catch. When paying for a cloud service offered by someone else, there are limits to the customization you can do. You sacrifice some control over functionality by choosing a cloud service over setting up your own on-premise infrastructure.

03

ON-PREMISE VS CLOUD

Security, Reliability, & Uptime

Whether you're choosing to utilize cloud applications or on-premise systems, data security will always be paramount. Data breaches can cause immense loss of revenue and loss of customer trust.

One of the most well-known examples of this is the 2017 Equifax data breach. This breach affected 148 million records, including social security numbers, birth dates, addresses, and in some cases driver's license numbers and credit card information, resulting in $700 million in damages to help people affected by the data breach, as well as reputational damage and congressional inquiries.

When cloud computing began to gain momentum, cloud vs on-premise security was a big question mark. Many organizations found themselves asking, "is the cloud safe for my data?" and "Will my information be safer in the cloud or on-premise?"

The cloud has historically been considered less secure than on-premise servers, but cloud computing is no longer a new technology. More and more organizations are discovering that the cloud can be a safe location for their data and processes.

In addition to a solution's security, reliability and uptime are essential factors when it comes to providing a good customer experience and maintaining productivity.

On-Premise Security, Reliability & Uptime

SECURITY

On-premise software requires that an organization purchase a license or a copy of the software to use it. Because the software itself is licensed and the entire instance of software resides within an organization's premises, they don't need to trust another company with their private data. Knowing that all your data is located within your in-house servers and IT infrastructure provides a certain peace of mind.

Companies that have extra sensitive information or are in highly regulated industries, such as government and banking, require the level of security and privacy that an on-premise solution provides.

With a local solution, the organization is responsible for setting appropriate user access policies, installing firewalls and antivirus software, ensuring security patches are installed promptly, and guarding against cyberattacks. If you have a strong IT department, you can rest easy. However, if mismanaged, on-premise servers can still leave your organization open to vulnerabilities and security threats.

RELIABILITY & UPTIME

On-premise installations are often considered to be more reliable; they're not dependent on external systems or network connectivity. However, if your server breaks or glitches, you have a problem. If a cloud server fails, your service provider can easily provision a new one. Setting up a redundant system for an on-premises solution is another story. Which means you could suffer a significant decrease in uptime if something happens to your on-premise equipment.

The phrase “Time is money” is attributed to Ben Franklin, and while he probably wasn’t talking about software uptime, it still applies. If your systems are down, you’re missing opportunities to reach customers. On-premise solutions don’t rely on sometimes finicky internet providers, however, they are limited by the number of servers you have on site. If your local server isn’t working properly, neither are you!

Cloud Security, Reliability & Uptime

SECURITY

Security concerns remain the most common roadblock to getting buy-in for a cloud computing solution. However, the gap between cloud vs on premise security is not as large as it used to be.

Today the largest cloud providers have robust security teams and tight procedures. Cloud security boasts a centralized core; with everything in one place traffic analysis is much easier and network monitoring takes a fraction of the time. In addition, cloud security tends to be highly automated thanks to APIs, which can make things easier on your IT staff. You may even be able to take advantage of specialized security options that would be too expensive to implement yourself.

On the other hand, using public cloud-based services requires trusting a third-party with your most precious data. Depending on how heavily regulated your industry is, you must ensure any provider you choose allows for compliance with necessary regulations. As some cloud-based security services come pre-configured, you may not have options for changes.

From personal information of employees, such as login credentials or social security numbers, to a loss of intellectual property, the security threats do exist and it’s important to understand what data is being collected and how a vendor will protect your data before implementing a cloud solution.

For example, let’s take a look at how Smarty, a primarily cloud-based address verification vendor, handles data privacy and security. Active PII (personally identifiable information) Redaction and Enhanced Data Privacy are two privacy solutions employed by Smarty.

Active PII Redaction

Smarty only needs an address file in order to parse, standardize and validate addresses. Their service doesn’t need any PII to validate an address and Smarty encourages users to send only necessary data.

In the event a user does include personally identifiable information in their address list, upon receipt, Smarty systems will seek out and eliminate any PII found. They look for data that is patterned like phone numbers, birthdays, social security numbers and emails and then redact the information prior to logging. That means no one can access PII from Smarty logs because it simply isn’t there.

03 ON-PREMISE VS CLOUD SECURITY, RELIABILITY, & UPTIME

Enhanced Data Privacy

Enhanced Data Privacy—commonly referred to as “incognito mode”—is an optional feature in the Smarty Platform that a user may elect to purchase. This feature prevents Client Data and/or PII from ever being logged at the point of submission or Provider’s APIs.

Client Data submissions are accessed only momentarily in Random Access Memory (RAM), just long enough to process and deliver results back to the client. Upon completion of the process, any residual Client Data in the system’s RAM is dumped or “garbage collected” and written over by subsequent transactions.

RELIABILITY & UPTIME

Cloud service providers can provide reliable service and high uptime because they can spin up new servers anytime the load increases or a server fails. You don’t need to buy any additional equipment or really take any action.

The flip side of that is that your company becomes dependent on the cloud provider. If support for a product is discontinued because a new version has been released, or if the cloud provider ceases operations, there’s not much you can do about it. You’ll have to look for a new solution.

In addition to reliability, uptime is a big selling point for cloud services. More uptime means less interruption in your workflow.

Here’s what typical uptime percentages mean in terms of your day to day productivity.

Availability %	Downtime/year	Downtime/quarter	Downtime/month	Downtime/week	Downtime/day (24 hours)
98%	7.31 days	43.86 hours	14.61 hours	3.36 hours	28.80 minutes
99%	3.65 days	21.9 hours	7.31 hours	1.68 hours	14.40 minutes
99.5%	1.83 days	10.98 hours	3.65 hours	50.40 minutes	7.20 minutes
99.8%	17.53 hours	4.38 hours	87.66 minutes	20.16 minutes	2.88 minutes
99.9%	8.77 hours	2.19 hours	43.83 minutes	10.08 minutes	1.44 minutes

Those decimal point differences might seem irrelevant at first, but as you can see, they make a big difference!

03 ON-PREMISE VS CLOUD SECURITY, RELIABILITY, & UPTIME

In order to understand exactly what you can expect from a cloud provider in terms of reliability and up-time, ask to see their Service Level Agreement (SLA).

An SLA defines specific aspects of the service provided and covers common metrics such as measurements of uptime and speed, as well as estimates of how frequently the provider expects downtime and how long it will take to restore service. In the agreement, the provider will detail which things are the company's fault, which things are not their fault, and what kind of compensation you're guaranteed if the company doesn't meet their own standards.

For example, Smarty guarantees sub-500 millisecond response times on address validation requests. That's the bare minimum slowest speed you can expect from their cloud services. Although they tend to average closer to sub-30 millisecond speed, what they're promising is sub-500 and you're not owed anything as long as requests are processed at least that quickly.

Other metrics you might see in an SLA include Mean Time Between Failures (MTBF) and Mean Time To Recovery (MTTR). What these represent, other than a tasty bowl of alphabet soup, are the lengths of time you can expect the service to work before breaking down, and how long it will take to get it back up and running so you can do your work. You can use these rates to see how different companies stack up against each other: a company with an MTBF of three days is less impressive than a company that has a MTBF of two weeks.

This is an instance where cloud providers can really differentiate themselves from on-premise solutions. Take Smarty, again. Their SLA doesn't have a listed MTBF time. Why? Because they have multiple, identical systems running in a number of diverse geographical locations across the country. You benefit from their fully-redundant system—backups on backups on backups! For most companies, it would be far too expensive to implement that much redundancy on premises.

But what if there is a lapse in service somehow? An SLA should also outline what recompense you'll receive for a lapse in service. The response usually depends on who is at fault.

- If the service provider is at fault: There will usually be a protocol for compensation, such as a credit to your account.
- If the client is at fault: Unfortunately, this is not a situation where the customer is always right...
- If neither is at fault: There will not be compensation, but the provider will likely give recommendations on how to avoid similar problems in the future.

Knowing what's covered in an SLA can pay off—and prevent a lot of uncomfortable calls with customer support. Don't be afraid to ask to see one, and then hold the provider to their promises if you choose them.

Pro Tip: When considering a vendor, ask them about historical uptime. That will give you a good idea of the kind of uptime you can expect if you choose to work with them. Check out Smarty's historical uptime here.

04

ON-PREMISE VS CLOUD

Compliance

Healthcare, insurance, pharmaceutical, energy, telecommunication, and banking operate as the most regulated industries in the United States.

Organizations in these industries must comply with strict rules and regulations at the federal, state, and sometimes even local, levels. Many of these regulations center around data management and privacy.

One of the most commonly known compliance regulations is HIPAA (Health Insurance Portability and Accountability Act of 1996), which created national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. GDPR is another common data privacy standard.

If you operate under one of these regulations or in one of the aforementioned industries, you might wonder if you can even consider moving to a cloud solution or if you're stuck with an on premise setup. There are certainly extra considerations if you want to maintain compliance in the cloud, but let's look at the differences between on-premise and cloud compliance before you give up on your cloud dreams entirely.

On-Premise Compliance

With an on-premise solution, you have all the control and can set up the exact security measures required.

Do you have a complex, custom data processing environment with specific security and compliance requirements? Would it be expensive to recreate all of those rules and controls in a cloud environment? In that situation, on-premise may be the right answer for your organization.

In addition, if you have an existing, mature, and secure on-premise environment, it may make sense to host any new systems on-site as well. It also allows engineers and architects to use tools and systems they already understand and work behind existing firewalls.

However, because you're maintaining your data and systems all in-house, it's up to you to implement compliance best practices, like monitoring logins, having clear security incident procedures, and using encryption. Implementing those procedures—and implementing them well—can be resource intensive.

Cloud Compliance

Systems and data are accessed and managed differently in the cloud versus on-premise, which means different methods of handling compliance are also required. One of the benefits of cloud vs on-premise is that you can look for a cloud vendor that's already been assessed and certified to meet compliance regulations and standards. Doing a search for specific security and compliance requirements relevant to your data should help you narrow down your search for a cloud provider.

However, this doesn't absolve you of the responsibility should there be a breach. Amazon Web Services (AWS), a well-known cloud service provider, established a concept known as Shared Responsibility Model for the cloud.

04 ON-PREMISE VS CLOUD COMPLIANCE

When it comes to cloud compliance, the Shared Responsibility Model means:

- Cloud service providers must ensure the compliance of their cloud-based infrastructure.
- Customers are expected to ensure the compliance of their own data, networks, applications, and operating systems that live in the cloud.

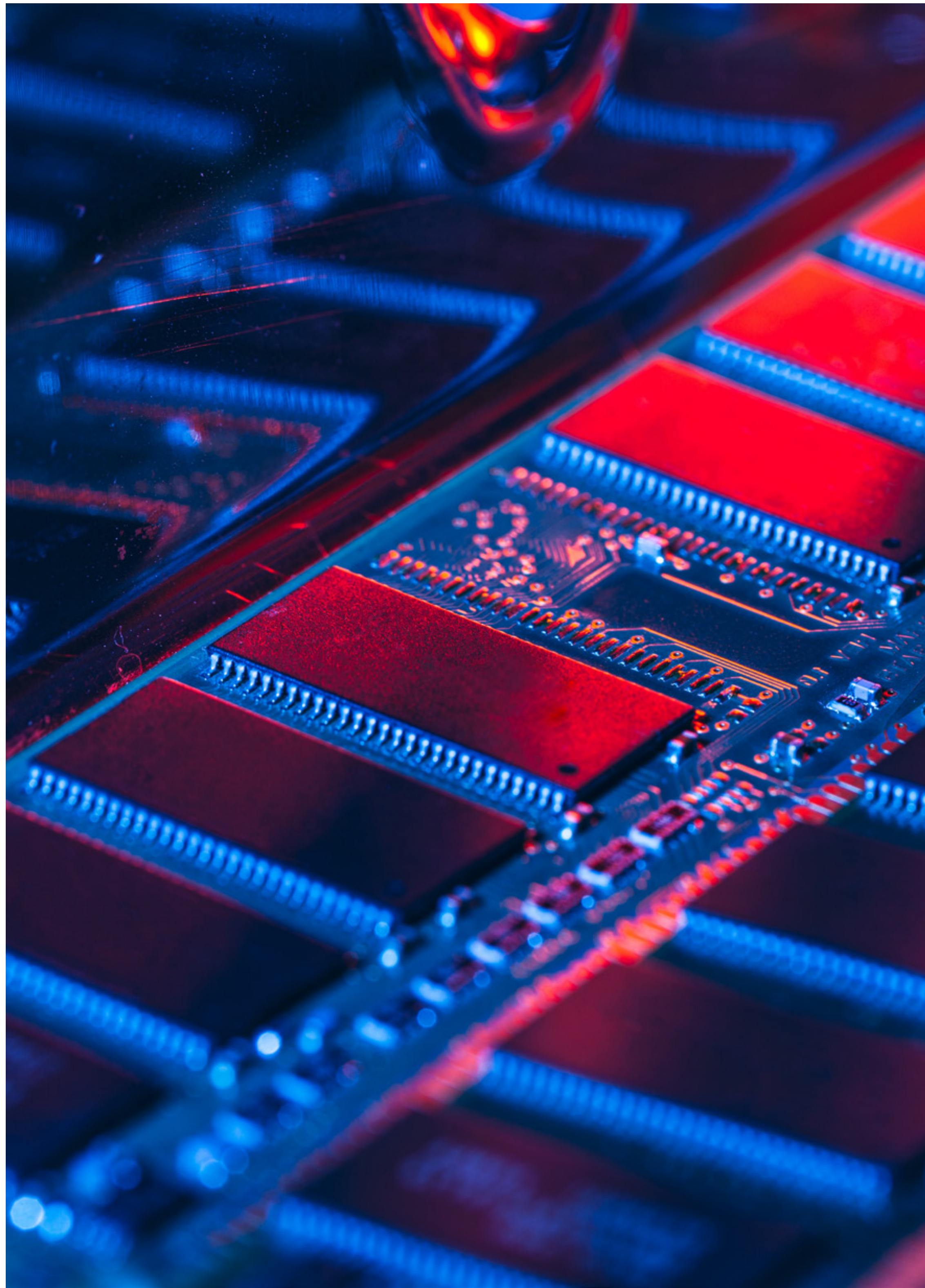
Let's use HIPAA compliance as an example. Covered entities (the healthcare organization) and their business associates, which a cloud service provider would qualify as, must both comply with the applicable provisions of the HIPAA Rules.

In these situations, a Business Associate Agreement (BAA) is made between the healthcare customer and the cloud service provider. This agreement affirms that both entities agree to hold up their end of the shared responsibility model in relation to compliance. In addition, a Service Level Agreement (SLA) is typically used to address the specific business expectations between a cloud service provider and their customer.

An SLA between a healthcare organization and a cloud provider might include provisions that address HIPAA concerns like:

- System availability and reliability
- Back-up and data recovery in case of ransomware attack or another emergency
- How data will be returned to the customer following service termination
- Security responsibility
- Use, retention and disclosure limitations

As the organization subject to compliance regulations, you need to understand the security procedures offered by a particular cloud service provider so you can make your own risk analysis and, if needed, establish risk management policies. Make certain that you ask for the cloud vendor's attestation reports and review them to understand where their controls might not be enough for your compliance obligations.



05

ON-PREMISE VS CLOUD

Total Cost of Ownership (TCO)

Companies often want to know “is moving to the cloud cheaper than on-premise solutions?” To fully understand the cloud vs on-premise cost comparison, you have to consider the total cost of ownership, or TCO.

TCO is a financial estimate intended to help buyers and owners determine the direct and indirect lifetime costs of a product or service. The concept was popularized by the Gartner Group in 1987 and remains important today for evaluating technology costs that aren’t always reflected in the upfront purchase price.

TCO includes: **purchase price, maintenance, and lifetime operational costs.**

The total cost of ownership for new software often includes training costs, hardware, implementation, customization and data migration, all in addition to the up-front software purchase cost. Determining your TCO is an essential part of calculating your return on investment (ROI).

The follow formula is a simple way to calculate TCO:

TCO = Capital expenditures (CAPEX) + Operating expenditures (OPEX)

So let’s take a look at the cloud vs on-premise TCO and find out if cloud really is cheaper than on-premise.

05 ON-PREMISE VS CLOUD TOTAL COST OF OWNERSHIP (TCO)

On Premise TCO

Building an on-premise system from the ground up takes effort, and often comes at a high cost. There's the initial investment into servers, infrastructure, and processes, and then there's the continued maintenance and ongoing operating costs.

The lifespan of physical equipment is about 3 – 5 years, meaning you'll need to consider equipment replacements in your TCO calculation.

Capital Expenditures: On-Premise

- Server purchase
- Storage costs
- Security devices
- Network
- Internet (IP)
- Software licenses
- Infrastructure design
- Backup system
- Datacenter colocation
- Redundancy to 2 data centers (if needed for disaster recovery)

Operating Expenditures: On-Premise

- Updates and improvements throughout lifespan
- Maintenance
- Technical support
- Staff training
- Energy consumption
- Constant temperature monitoring
- End of life disposal
- Equipment replacement

Cloud Cost TCO

Cloud services are typically priced on a pay-as-you-go approach, which eliminates many of the up-front capital costs of in-house solutions. Implementation is much cheaper and faster and you don't need to buy servers or rent space at a datacenter, or maintain your own security procedures.

A cloud solution eliminates many operating costs, as well. Your company isn't paying for updates and maintenance or worrying about temperature monitoring; that's all performed by the cloud host. You may still need to factor in training your staff to use the new solution, and possible support fees from the provider when you have questions. However, most organizations find that by migrating to the cloud they experience a significant TCO reduction.

Calculating all this might seem like overkill, but after doing a cloud vs on premise cost comparison, your choice of on-premise vs cloud storage or other software solutions may be very apparent.

06

ON-PREMISE VS CLOUD

Vs Hybrid

Throughout this ebook, we've been focusing on the differences between cloud and on-premise software. And for many years, cloud versus on-premise has been the main debate. This is the part where the infomercial spokesperson shouts, "But wait, there's more!"

There is a third option that's been emerging in popularity: hybrid cloud.

A hybrid cloud environment uses a mix of on-premises infrastructure, private cloud services, and public cloud services—such as Amazon Web Services (AWS), Microsoft, or Google.

The primary benefit of a hybrid cloud is agility. Organizations can move between private IT environments or public clouds as computing needs and costs change. For example, sensitive data could be kept on-premise or in a private cloud, with less critical workloads hosted in a public cloud.

What is a private cloud? A private cloud is a cloud environment that's accessed and used by only one client. The main difference between private cloud vs on-premise solutions is that private clouds can be located within an organization's data center (aka on the premises), or located off-site and managed by a third-party.

Before you move to a hybrid cloud solution, you need to have the technology in place to allow the two solutions to connect and interact. A strong network connection is essential to a successful hybrid cloud strategy. This usually means a wide area network or dedicated networking service for additional security.

Hybrid cloud can seem like the best of both worlds because it offers both security and scalability. It is, however, more complex than a traditional cloud SaaS model, and therefore more expensive.

Pondering cloud vs on-premise vs hybrid? Here are some common business cases where a hybrid cloud solution works best:

- Temporary processing needs or highly changeable workloads: A hybrid cloud solution is particularly beneficial for organizations with highly changeable workloads. For example, transactional order-entry systems that experience significant seasonal demand spikes—like zoo concession stands or theme park ticket sales—are good hybrid cloud candidates.
- Disaster recovery for essential workloads: While this will increase your management complexity, you can use a hybrid cloud solution to replicate your on-premise workloads and back up data to the cloud. This way, if there's a disruption to your data center, workloads will fail over to the cloud environment and continue to operate via on-demand cloud resources.
- Digital transformation or moving to the cloud at your own pace: Hybrid is a good way to dip your organizational toes into the cloud. Put some of your workloads on a public cloud or on a small-scale private cloud. Evaluate what works for your enterprise over time and you can then expand your cloud presence as needed.

Conclusion

As you can see, many factors go into the cloud computing vs on-premise debate. Ultimately, what you choose will depend on your company's specific needs, but now you're ready to make that decision armed with all the facts. We've included a handy chart at the end of this eBook that summarizes each key factor in the on-premise versus cloud software debate.

	On Premise
Deployment	Deployment is done in-house using your staff and your company's tech. On-premise implementations take longer due to the time needed to complete installations on servers and any individual computers or laptops.
Control	On-premise deployment gives you complete control. Your data, hardware, and software platforms are all yours. You decide on the configuration, the upgrades, and system changes.
Agility	Scaling your on-premise infrastructure up or down would require additional time and expense. You cannot make changes quickly and you're committing a lot of IT hours to the internal upkeep of the hardware, software, data backups, storage, and disaster recovery.
Security	Because the software itself is licensed and the entire instance of software resides within an organization's premises, you don't need to trust another company with your private data. Knowing that all your data is located within your in-house servers and IT infrastructure provides a certain peace of mind. However, you need a skilled IT department to implement the best security measures.
Reliability	On-premise installations are often considered to be more reliable—they're not dependent on external systems or network connectivity. However, if your server breaks or glitches, you have a problem. It is expensive to set up redundant systems for on-premise infrastructure.
Uptime	On-premise solutions don't rely on sometimes finicky internet providers, however, they are limited by the number of servers you have on site. You could suffer a significant decrease in uptime if something happens to your on-premise equipment.
Compliance	You have all the control and can set up the exact security measures needed. However, because you're maintaining your data and systems all in-house, it's up to you to implement compliance best practices, like monitoring logins, having clear security incident procedures, and using encryption.
TCO	Building an on-premise system from the ground up takes effort, and often comes at a high cost. There's the initial investment into servers, infrastructure, and processes, and then there's the continued maintenance and ongoing operating costs.

	Cloud
Deployment	Cloud services can be deployed over the internet in a matter of days, hours, or minutes— even seconds!—because nothing needs to be installed on a physical server or computers.
Control	Access to the physical server is restricted but control of hardware is maintained through the different cloud providers' user interfaces as well as software.
Agility	Agility is a key characteristic of cloud services. It's easy to scale cloud services up and down and the ease of implementation means you can easily roll out new functions.
Security	Cloud security tends to be highly automated thanks to APIs, which can make things easier on your IT staff. Traffic analysis is easier and network monitoring takes a fraction of the time. On the other hand, using public cloud-based services requires trusting a third-party with your most precious data and as some cloud-based security services come pre-configured, you may not have options for changes.
Reliability	Unlike on-premise servers, cloud solutions can quickly spin up new servers anytime a server fails. Thanks to that redundancy, your work can continue without disruption.
Uptime	Hardware, software, configuration, and network access can all impact uptime. A high capacity infrastructure, or a cloud service that scales to meet demand, can increase your uptime. When considering a vendor, ask them about historical uptime. That will give you a good idea of the kind of uptime you can expect if you choose to work with them.
Compliance	One major advantage of switching to the cloud is that you can look for a cloud vendor that's already been assessed and certified to meet compliance regulations and standards. However, the Shared Responsibility Model dictates that it's up to both you and your cloud service provider to ensure compliance with the relevant regulations.
TCO	The upfront cost of a cloud service is much lower and implementation is faster. You don't need to buy servers and your company isn't paying for updates and maintenance. You may still need to factor in training your staff to use the new solution. However, most organizations find that by migrating to the cloud they experience a significant TCO reduction.

Discover even more business benefits
of location data intelligence at:

smarty.com

smarty