PENTA

THE TRUE COST OF CLOUD COMPUTING IN 2025 — AND THE ALTERNATIVES

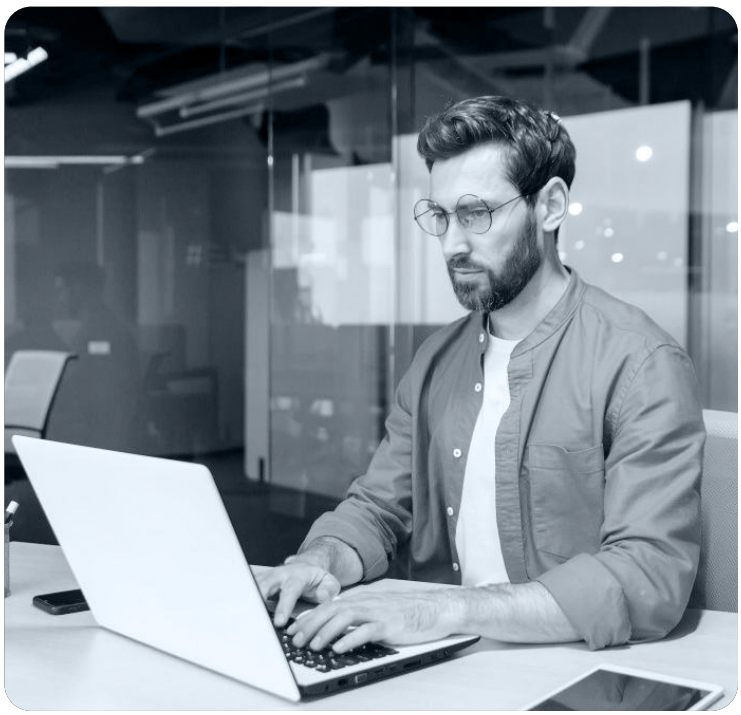
White Paper

Cloud computing has transformed the possibilities for managing IT infrastructure, and businesses are keen to capitalise on the benefits. Here's what anyone making cloud decisions needs to know.

Table of Contents

Overview: Where we are and how we got here

During the cloud craze ten years ago, you were told that moving to public clouds (like Amazon and Azure) would yield huge cost and complexity savings. But even now, in 2025, those promises have—for the most part—yet to be fulfilled. **And to add salt to the wound, hosting costs are ballooning, unpredictable, and come accompanied by expensive IT engineer retention fees.** If all this makes you feel like you've been sold up the river, settle in, because there's more...



83%

of businesses consider cloud "extremely important" to their future strategy and growth, according to a recent report from Splunk and Harvard Business Review Analytic Services.

50%

of corporate data is stored in the cloud

20%

The year-on-year growth rate of public cloud spending predicted by Gartner

Cloud is now a mainstream technology, with potential applications across the entire corporate spectrum from HR to sales to C-suite. And when tech goes mainstream, businesses who don't harness it will eventually find it impossible to stay competitive.

In other words, the pressure to partake in the cloud is on.

However, large-scale solutions are often complex, and cloud computing is no exception. While it's true that it's a busy market, where it's easy to get overwhelmed and potentially make a sub-optimal choice, that's not the main issue here.

Key cloud challenges

Greater complexity

The market is frankly overloaded with services and solutions. Being spoilt for choice is supposed to be a positive, but with it comes overall network complexity. The reality for businesses is that their applications and services are located across a variety of cloud environments.

This makes it hard to pin down the exact causes of IT issues when they occur. Nearly half of companies said that cloud deployments were **more complicated than they expected,** and nearly half of C-suite executives said that **complexity could have significant, negative impacts on cloud ROI** over the next five years.

Vendor lock-in

The IT is often so complex that shopping around once you're committed is nothing short of a nightmare. And if you want to do it properly, the process takes so long that you're essentially destined to be in a perpetual migration cycle.

Increased attack surface

More cloud data and more cloud services mean that **threat actors have more options for attacks.** It's true that on-site data is hardly safe either, but it's safe to say that cloud security is a considerable challenge. The scale of many businesses' cloud operations also means that it's hard to pin down the nature and location of the attack.

OVER 50% OF ALL CLOUD THREATS ARE RELATED TO RANSOMWARE

Less visibility

As adoption of cloud services increases, visibility will, on the whole, decrease. The readily available **self-service options only add to the challenge**, because it means staff can quickly spin up instances and services on demand, making it **hard for IT teams** to keep track of everything.

The fallout includes paying more than they need to, or unmonitored services being compromised. In 2022, **businesses took on average around 9 months to discover a breach,** according to IBM, and with cloud adoption ramping up, this could potentially increase.

Expertise shortage

Cloud services may individually reduce the burden on IT teams, but collectively they need the oversight and management of skilled specialists. This need only widens the existing IT skills gap. **Lack of in-house cloud expertise is a serious challenge,** with many businesses turning to investment in training in order to upskill existing staff.

It takes businesses 9 MONTHS on average to discover a breach

Emerging tech

IT's evolution never takes a break. Cloud environments are constantly seeing new security tech, and networking advancements.

These new iterations offer benefits, but they require IT teams to get familiar with new tools or configurations.

To add to the challenge, the pace of development for user-facing tools is often much faster than security, meaning **protection may not be able to keep up with productivity.**

All these challenges add up to a sizeable gap between the potential and the reality of the cloud. It's important for all decision-makers to go into any cloud selection process with their eyes open to these hurdles.

BUT GOOD NEWS: this whitepaper will demystify, analyse and compare the three main options for cloud: **PUBLIC CLOUD, SELF-HOSTED PRIVATE CLOUD, and MANAGED PRIVATE CLOUD.**

Consider this whitepaper your cloud compass of sorts

WE'LL LOOK AT:

- **The characteristics of these three cloud models**
- **The cost implications of each option**
- **The security pros and cons of each model**

By the end, you'll feel equipped to make a more informed decision that fits with your business's specific needs.

You'll feel more confident in unlocking the full potential of the cloud.

But just before we dive in, it's worth getting the definitions locked down...

Cloud models: definitions and key terms

We want this guide to be accessible not just to IT professionals, but those whose expertise lies in other areas, but who are facing a cloud selection process.

Therefore, we want to make sure we're all on the same page when using certain terms.

Public cloud:

This is where providers like AWS, Google Cloud and Azure offer resources such as storage, servers and databases. It's a shared data centre, and you usually pay as you go.

Private cloud:

A dedicated cloud environment, usually designed specifically for the organisation it serves. In this whitepaper we'll be covering both self-hosted and managed private clouds.

On-premise:

The traditional, old-school setup. This is in-house infrastructure, featuring physical servers and storage, all managed by the organization.

Self-hosting:

In short, this refers to managing your own IT infrastructure. This doesn't mean the infrastructure's on-premise though, just that you're responsible for everything, from hardware to software.

Virtual machine (VM):

A VM is a simulated computer system that runs on a server.
Just like a physical computer, it can be configured with its own operating system, storage and memory. Cloud providers can assign numerous VMs to suit the needs of the organisation.

Scales in the sky: Weighing up the cost of cloud

Cloud computing has financial advantages in that **you can avoid certain costs** of facilities and equipment maintenance.
However, it's not unusual to get stung by unexpected charges. Therefore, it's vital to understand how cloud computing's pricing is affected by its different uses, to avoid a surprise dent in your bottom line.

This isn't a cost calculator—though they do exist. Determining the exact costs across the three core options is difficult without specifics. There are a lot of variables, a lot of moving parts, and costs can change day by day.

COST PROS AND CONS OF CLOUD MODELS

Public cloud

Cost advantages

Public cloud is often pay-as-you-go, so you only pay for what you use, in terms of storage and computing power. If your workload fluctuates, this can be the most cost-effective option.

There are no upfront hardware costs. You don't need to buy servers and storage devices, and you don't need to find or build a location for them.

If you're starting out, scaling up isn't an issue. Equally, if you're streamlining or shrinking operations you can scale down accordingly and make savings.

Cost disadvantages

Variable usage patterns will result in variable costs...which is fine unless you find your usage is higher than expected, and therefore so are the costs.

Customers talk about vendor lock-in being a challenge. It's not always the easiest to transfer out of the public cloud—and it's well worth noting that some providers charge for transferring client data out of the cloud.

Public cloud security is strong, but in some industries, regulations will demand that organisations use self-hosted or managed private cloud as these options are seen as offering superior control.

Self-hosted private cloud

Cost advantages

Self-hosted cloud has the potential to be lower-cost in the long term—if used efficiently.

Organisations retain complete control of their cloud environment, including data and infrastructure.

Cost disadvantages

The upfront costs are considerable. You will need to purchase servers, storage, software licences and networking kit, as well as lease data centre premises.

There will be ongoing costs for hardware upgrades, renewing software licences and a team of IT professionals to manage and maintain the cloud. And don't forget electricity, air conditioning and the entire tech stack.

If you need to scale up, it can be slow and expensive.

Managed private cloud

Cost advantages

Fixed, regular fees can make it easier to budget. Costs are more predictable, making budget planning easier.

There is less burden on the organisation, as the provider manages and maintains the cloud.

The ability to share services, hardware and licenses with other hosted clients (depending on your configuration requirements). This could include high bandwidth internet lines, firewalls, email servers, and even security measures.

Cost disadvantages

Costs can be higher than a public cloud, if you're paying for a dedicated environment.

As with public cloud, there's a risk of vendor lock-in, as switching providers may attract migration costs.

How do providers determine cloud costs?

What goes into the costs charged by cloud providers? Some key factors are:

- **Networking:** Maintaining the network, including the costs of hardware, network setup, maintenance, and people to do the work.
- **Storage:** Operating an organisation's storage hardware, and/or buying new hardware to meet the customer's storage requirements.
- **Computing:** The costs associated with VMs, CPUs, licensing fees for any software where applicable, and virtual RAM.

Cost comparison
Mid-size server infrastructure – up to 130 VMs per client

Stacking for success: A tech stack comparison

To choose the right cloud model for you, you need an understanding of the technologies that underpin each one. But even more important when choosing the best fit, **you need to take into account exactly what you'll need to manage.**
So, let's take a look at each option:

Public cloud

Providers are responsible for managing the underlying infrastructure. Physical servers, storage, network—they take care of it all. They offer pre-configured environments for running apps and databases, all as part of their range of platform-as-a-service (PaaS) options.

Public clouds have a large selection of applications to meet an array of business needs. This might include tools that handle customer relationships and productivity. As a customer, you can use these through a web browser, meaning you don't have to manage the related infrastructure. Access to applications may be given as an optional extra rather than standard.

Similarly, public cloud offers management tools that can monitor performance and keep tabs on costs. Again, these tend to be web-based. In terms of security, public cloud providers are mindful of the service being shared.

Therefore they put a lot of resources into a solid security structure. They also offer a range of security services so that their customers can keep in line with any data protection and compliance requirements.

Self-hosted private cloud

As the name implies, organisations who opt for self-hosted private cloud will need to buy and manage their own physical servers and networking equipment.

Platforms are optional with private cloud, but some organisations will opt for open-source platforms (like OpenStack or CloudStack). This opens up some self-service options.

Organisations get the full choice of which software's on their self-hosted private cloud. Custom applications, open-source software, and commercial software licences—anything goes. The same can be said for management tools. Organisations choose and manage everything to do with managing resources, security and resource management.

When it comes to security, the buck stops with the organisation. They are solely responsible for securing their self-hosted private cloud, and for making sure it's accessed by only authorised people.

Managed private cloud

As with a public cloud, a managed private cloud is provided and managed by a third party. But unlike a public cloud, this cloud's infrastructure is dedicated to a specific organisation.

Typically, managed private clouds offer a pre-configured, PaaS-style platform. Customers' level of choice for software will vary depending on provider. Some will offer popular options, but others focus purely on managing the infrastructure.

When it comes to management tools, managed private clouds tend to be fairly user-friendly. That said, the customisation options will likely not be as carte blanche as a self-hosted private cloud.

Security is a team effort with this option. While providers of managed private clouds will look after the infrastructure, organisations will be responsible for ensuring that their data and applications are secure.

The best tech stack for you depends on your specific needs, and your top priorities. It also depends on your regulations, the amount of technical expertise you have to hand (or are willing to recruit), scalability needs, and your budget.

Clear skies, clear costs: From sticker price to TCO

As we discussed above, the cost of VMs varies, as does cost per TB. But this is only part of the total cost of ownership, or TCO.

The TCO is best visualised as the building blocks of cloud infrastructure, from electricity and cooling, to hardware, various abstract layers like operating system and network, right through to end-user support.

This is important to understand, because the focus can be solely on the cost of the solution that the vendor is offering. But this is just the tip of the iceberg.

What not everyone appreciates at the time of choosing a cloud model is that a **public cloud solution only covers some of the elements.** It's not a complete solution; **you still need engineers to manage it**—and that means you also need staffing backups and other costly things that all too easily get overlooked.

TCO needs to be front of mind when choosing a cloud model. Be aware of all the elements needed to supply an IT service, and their cost. If you're not aware of all the elements, you will likely overlook the real TCO.

THE TCO INCLUDES:

- **Infrastructure cost e.g. network, storage, CPU, colocation, software**
- **Purchase costs and taxes**
- **Interest component**
- **Funding and incentives**
- **Maintenance costs**
- **Support costs**
- **Energy costs**
- **Replacement costs**
- **Staff costs**

Lifting the cloud cover: Exploring the strategic advantages

Above, we compared cost pros and cons for the three core options of cloud. But, widening our focus, each comes with its own distinct strategic advantages. There is no overall winner here—it comes down to your preferences and needs on a number of factors, from agility to security to storage options.
Let's explore the strategic advantages of different cloud models.

Public cloud

Public clouds are perhaps most loved for their cost-effective tendencies: **Only pay for what you use, on a pay-as-you-go basis, and avoid the heavy setup costs of self-hosting.**

Public clouds enable businesses to scale their infrastructure to suit, increasing or reducing cloud provision to match their operations.

The technical innovation of public clouds can be impressive too. **Heavyweight providers, like Amazon Web Services (AWS) and Microsoft Azure, have some of the best research and development teams out there.** Such names are constantly striving and competing to be at the cutting edge of cloud solutions. They boast options like artificial intelligence (AI) components, advanced analytics, and machine learning.
This means—much like the cloud hardware—businesses don't need to invest in do-it-yourself solutions.

The appeal of opting for public cloud providers doesn't stop there: many have a global reach, which allows their clients to deploy data and tools across the world, wherever needed. This can help ensure continuity and mitigate any mishaps. With a single hour of downtime costing **44% of enterprises over $1 million,** the benefits of business-as-usual cannot be overstated.

Of course, no cloud model is without its downsides. At the top of that list are security concerns. While providers work hard to ensure robust security, **public clouds are shared spaces.**
And just as there are considerations for a building shared between multiple businesses, there are potential risks of sharing digital space too. Clients may have concerns about data privacy and compliance, and—as we touched on earlier—for some industries, a public cloud may be incompatible with regulations.

The per-minute pricing structure of everything is highly profitable for cloud companies, which might go some way to explaining why Amazon's AWS is the most profitable part of the whole business—the margins are huge.

Private managed clouds

Private managed clouds can be a compelling “best of both worlds” option. They combine the flexibility and pocket-friendliness of public clouds with the enhanced security and control of self-hosted clouds.

With this option, a dedicated environment houses the cloud infrastructure. This environment is completely separate from other clients of the same provider. This means your data and infrastructure is more secure —which is particularly useful if you handle a lot of sensitive data or if you have stringent industry regulations.

What’s more, the predictable costs of private managed clouds are a definite benefit. Clients pay a fixed monthly fee for a particular service level, which gives them greater budget control compared to the public cloud model.

From a resources point of view, it’s a plus point that managed private clouds and maintained by the provider’s personnel. This means the client’s existing IT team isn’t over burdened, allowing them to prioritise the projects that are central to the organisation’s goals. IT teams in both organisations can both communicate and collaborate closely, which is simply not possible in public cloud.

Self-hosted private clouds

For some organisations, granular control and the highest security are paramount. It’s such organisations that would find a good fit in self-hosted private clouds. Here, the organisation owns and operates the whole cloud, giving complete control over hardware, software and security.

But, as we mentioned, this ultimate level of control comes at a significant cost. Building and maintaining such an infrastructure takes huge effort, a large investment, the right people, and time.

Further, when it comes to scaling, this model presents the biggest challenge as it’s down to the organisation to put in place additional storage, infrastructure and personnel as needed. Compared to the instant provisioning of managed options, this can make self-hosted models less appealing.

As a very rough guide, for every dollar an organisation spends on capital expenses to upgrade its IT infrastructure, it can expect to pay an additional two dollars to manage, maintain and secure that infrastructure.

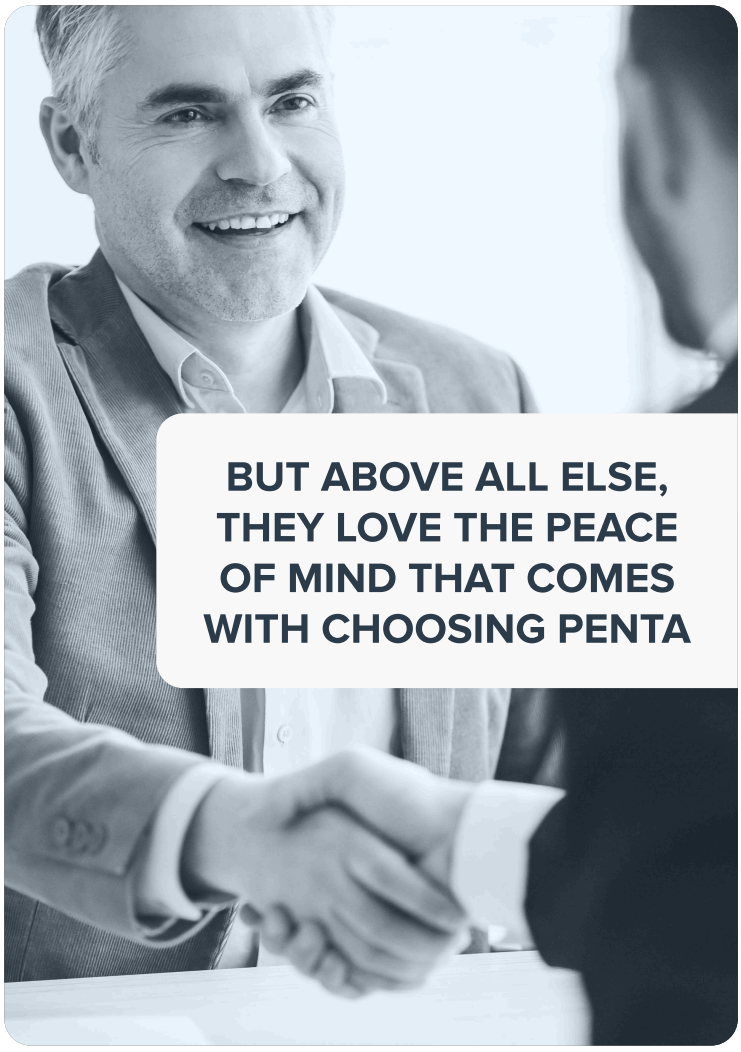
Penta: Secure, scalable solutions to help your business soar

This will never be a straightforward decision. We can't climb this mountain for you.

Each model offers distinct advantages—and drawbacks.

And, as with so much in life, the best cloud option for your business depends on your needs, and on things like:

- **The size and predictability of your workload**
- **Your security needs**
- **Your IT business's in-house IT expertise**



Penta: Secure, scalable solutions to help your business soar

We know that today's businesses exist in an extraordinarily dynamic landscape. And we understand the complexities of the cloud.

That's why Penta's cloud services are designed for maximum efficiency and agility, without compromising security.

Our clients love the personalised approach we take. They're delighted by the way our team of experts work closely with them to assess their needs, design a secure cloud architecture, and provide ongoing support to ensure their data is always protected.

So if you're ready to take your business to the cloud, Contact Penta today and explore how our cloud services can supercharge your success.

PENTA

Europe
GENEVA, SWITZERLAND

sales@penta.ch | **+41 22 316 1000**

Rue Bémont 4, 1204
Geneva, Switzerland

The Middle East
DUBAI, UNITED ARAB EMIRATES

sales@penta.ch | **+971 4 376 7100**

607, Innovation One,
Dubai International Financial Centre (DIFC),
Dubai, (UAE)