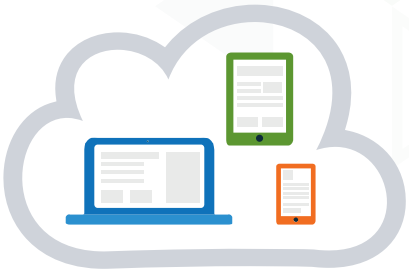
druva

Executive Brief

Making The Case for the Cloud: Comparing Cloud vs On-Premise Deployments

This paper is for IT professionals choosing between an on-premise or cloud-hosted deployment for data availability and governance.

Choosing the right deployment model for your company's data availability and governance implementation is essential. Obviously, that's true from a financial standpoint; you want to make the most of your investment. But we -- you and we at Druva -- also want the deployment to be a huge success, and to create an environment that plasters a big smile on your face. So together we aim to ensure your deployment has adequate security protection and data availability.



Druva supports both on-premise and cloud deployments for inSync. While we have our technical preferences in general, it's most important to us that you get the best fit for your organization's specific needs.

In most cases, we've found, enterprises benefit from deploying inSync in a cloud environment. We're well aware that this view is not always a popular one, particularly in IT organizations where the executives have had a focus on data centers and an inherent distrust of cloud computing. Making the transition to cloud computing can be tough.

However, while we always do our best to support a customer's unique needs, expect us to give you a list of arguments to convince your organization that a cloud deployment is the way to go. That's what we aim to do in this document. Because we've found that many of the reasons for preferring deployments to be on-premises come down to a perception that "cloud means giving up control of one's data." That's not the case. When done right (and we do know how to do it right!), the cloud isn't one-size-fits-all. It's elastic, it's configurable, and it avails itself to the sort of adaptation global enterprises need.

So let us back up our assertion, and we can see if you come to view things our way.

Enterprises are traditionally very good at managing back-office applications and building multi-tier architectures. However, few large organizations have the experience or resources required to build software architectures that depend on high scalability and massive parallel processing. So why build your own data center when you can just go out and get one?

There are some common assumptions (or shall we call them myths?) about on-premise deployments versus a public cloud deployment, and opinions can vary greatly across a range of viewpoints.

Among these assumptions:

- A private cloud is more cost-effective than a public cloud option.
- A private cloud gives us sufficient elasticity, better than public cloud options.
- Private clouds are more flexible in serving our unique needs.
- Private clouds are more secure and more compliant than the public cloud.
- A private cloud has better disaster recovery (DR) and/or reliability than the public cloud.

Despite these commonly held viewpoints, we have found that a public cloud deployment makes sense for most inSync users. Here's the top five reasons why customers are choosing public cloud deployments:

1 Cost Effectiveness

Objection: A private cloud is more cost-effective than a public cloud option.

The debate is waged daily between *operating expense* (a.k.a. OPEX, the cloud's approach) and capital expense (a.k.a. CAPEX, the on-premises approach). Cost or expenditure outlays can be capitalized (spread out over a period of time) or built into a specific time period's profit/loss (the time period during which they were incurred).

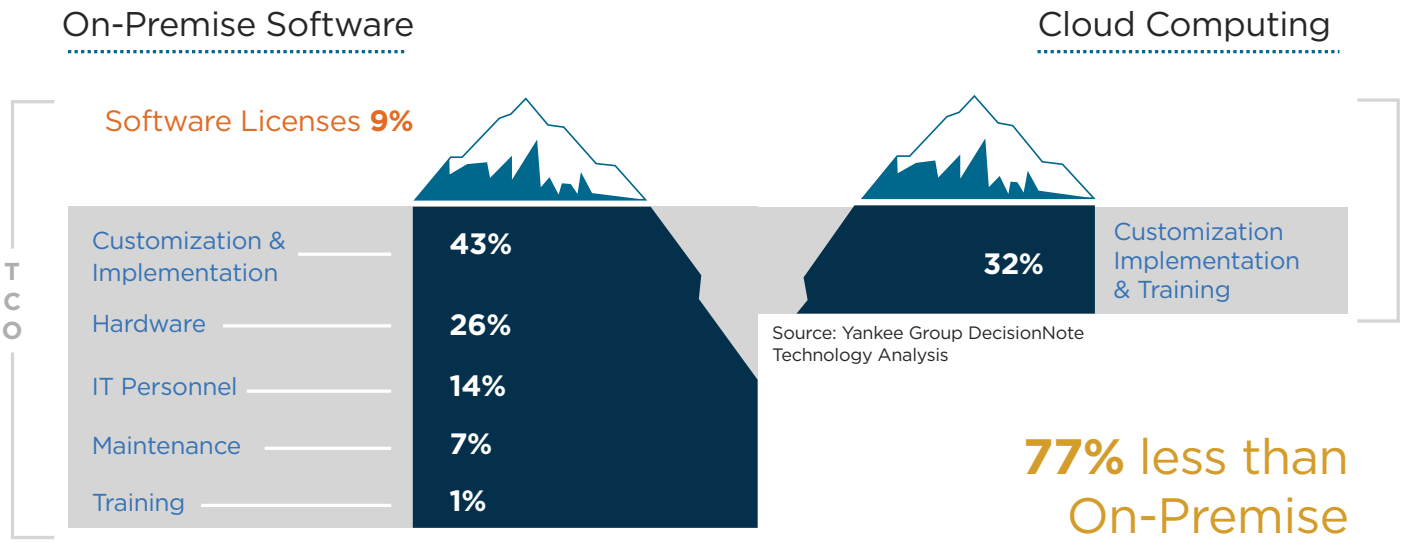
Although there are trade-offs to each option, OPEX is increasingly favored by finance departments. In the age-old rent-versus-buy debate, the cloud is making rental very compelling. Cloud computing is much faster to deploy. Businesses have minimal project start-up costs, predictable ongoing operating expenses, and they pay only for the capacity they need right-now, with the ability to scale as their requirements change.

A recent study conducted by Forrester Research investigated the cost avoidance savings for on-premises solutions by companies that had implemented inSync in the cloud. As Forrester reported, one global pharmaceutical firm estimated that inSync was 60% cheaper than the storage infrastructure it would have bought. The enterprise estimated that inSync saved at least $1.5 million, based on the organization's estimate for the upfront costs to upgrade its legacy on-premise environment. If they had stuck with the on-premises environment, the enterprise also expected to incur additional staffing costs for three people to manage it.

2 Economies of Scale

Objection: A private cloud gives us sufficient elasticity, better than public cloud options.

No private cloud can compete on price with the likes of public cloud service providers such as Amazon Web Services (AWS) and Microsoft Azure. Plus, the public providers are constantly investing in R&D that leads to technological innovations that directly impact their public cloud's cost structures; it's their rate of innovation and development where the true economies of scale reside.



The ability to scale on demand (in both storage and compute power) is one of the biggest advantages of cloud computing. When you need more resources, you get them immediately. When you don't, you don't pay for anything you don't use. And you don't have to install new hardware or infrastructure on the off-chance it's needed, or for the worst-case scenario. This allows organizations to support business growth without expensive changes to existing IT systems.

In traditional on-premises deployments, often IT capacity decisions have to be made prior to deploying an application. IT managers must guesstimate the right balance between sitting on expensive idle resources and dealing with limited capacity (and whiny users) during heavy traffic spikes. With any on-premise solution, you pay for all of the servers and infrastructure you *might* need, even if your current need is lower. You might pay for capacity that never gets used. Whereas a cloud deployment allows a more granular approach.

For on-premises implementations, scalability and elasticity are often equated with investment and infrastructure. IT managers have to provision resources up front for applications with variable consumption rates (such as backup, which of course is where Druva puts its attention). Imagine what would happen to a traditional IT shop if traffic to an application doubled or tripled in a short period -- or perhaps you don't need to imagine such a scenario. For example, during HR benefits' open enrollment periods, many corporate users generate significant traffic to internal applications. Your existing infrastructure has to handle a spike in traffic without interfering with normal business operations. Often, that means building systems for the worst-case scenario. Sometimes you can predict them, as with this oft-used HR benefits example; other times, you're surprised. Nobody likes those surprises.

One of the best features of cloud computing is that you use what you need -- whenever you need it. That gives you *more* control, not less. In the cloud, scalability and elasticity provide opportunity for savings and for improved ROI.AWS uses the term *elastic* to describe the way computing resources stretch to accommodate demand for projects with variable consumption rates or with short lifetimes.

In short: Instead of acquiring hardware, setting it up, and maintaining it in order to allocate resources to your applications, Druva inSync deployed in the cloud allows users to scale on demand to suit your needs.

3 Business Speed and Flexibility

Objection: Private clouds are more flexible in serving our unique needs.

Ofttimes, it's easier to let everything continue "as is" in the data center with little change to the IT architecture. But, as the business grows and changes (whose doesn't?), the data center has to grow and change, too. There's no longer a possibility of doing things the "old way that always worked," no matter how tech- or business-process-nostalgic we are.

If the current facility becomes a constraint, then it has to be replaced -- never the best option under any financial conditions. Therefore, something else has to provide the flexibility that IT and the business demand. Most of the time, the cloud is the best way to respond to that change, since it gives you *more* control over the data, and how it's stored, accessed, and safeguarded.

In a cloud computing environment, new IT resources are only ever a click away, which means you reduce the time it takes to make resources available. Instead of asking IT and developers to work together to provision servers, a process that can take weeks, resources are available in just minutes. This is beyond, "the organization has control" but rather an advantage for the human beings who aim to further the company's goals: "Let me just get my job done, so the right data gets in the right hands, soonest!"

An immediate concern for enterprise computing, these days, is the burden of controlling where data is stored. Do you have one data center in Germany, another in England, yet another in Des Moines? Data residency requirements mandate

compliance with industry and governmental agencies, such as ITAR and Europe's Data Protection Compliance regulations. With cloud computing, administrators can map users via profiles to regions, ensuring data resides in the location required by regional law.

4 Security & Compliance

Objection: Private clouds are more secure and more compliant than the public cloud.

The biggest security risk in any infrastructure is overlooking serious security flaws because of time, expertise, and resources (or the lack thereof). It's understandable -- and appropriate -- for IT managers to be concerned about access to cloud data, and to pay attention to security vulnerabilities. The reality is that a well-staffed cloud provider, with highly-trained staff who are dealing with security every day, may be better equipped to reduce the chances of security breaches occurring, compared to an overworked and under-resourced corporate IT department.

Really, you could spend less time conducting security reviews on infrastructure. Mature cloud providers have teams of people who focus on security, relying on industry standard best practices to ensure you're compliant. For example, AWS data centers feature numerous industry certifications, including SOC1 (Covers SAS-70 Type II, SSAE-16) and ISO-27001 as well as use state-of-the art electronic surveillance, multi-factor access control systems, and 24x7 physical security guards. Those Amazon data centers' environmental systems minimize the impact of disruptions to operations, backed up by multiple geographic regions that are equipped to cope with failures such as natural disasters, system failures, or zombies. (Well, perhaps not the zombies.)

In fact, security and compliance are why some of our most highly regulated customers such as Pfizer and Shire, have decided to deploy inSync in a cloud environment rather than on-premises.

5 Disaster Recovery & Reliability

Objection: A private cloud has better disaster recovery and reliability than the public cloud.

Planning for business continuity in the event of a power outage, fire, flood, zombie apocalypse, or other disaster is expensive and challenging. It requires investments in redundant infrastructure and staff across multiple data centers, costly storage replication solutions, and is typically reserved for larger enterprise that can afford investing in disaster recovery (DR).

In an inSync cloud deployment, we achieve availability by replication of your data in different AWS availability zones (distinct regions engineered to be insulated from one another) to ensure swift recovery in case of disaster. The service runs within Amazon's proven network infrastructure and data centers designed to 99.999999999% durability (that's measured in *seconds* of downtime per year) and a commitment (backed by a service level agreement, SLA) of 99.95% availability for each Amazon region.

Summary

While the reasons for choosing a cloud deployment over a on-premise deployment are pretty clear, the perceived notion of giving up control of one's data can be difficult for CIOs to accept. But with a reliable cloud service provider (guaranteed by rock-solid SLAs), companies have *more* control, not less. Delegating responsibility to a cloud service provider means that someone is motivated to ensure that everything is working properly. If it doesn't give the best, most flexible, most secure service, the provider doesn't stay in business. As the role of the CIO evolves to become more of a business enabler at the end of the day, CIOs need to remind themselves it's not what's good for IT that matters: It's what's good for their business and users.

CONSIDERATION	CLOUD	ON-PREMISE
IT Infrastructure	Limited or no internal IT resources and/or no desire to invest in or support additional IT infrastructure.	Established IT support with software domain expertise and a solid backup and security strategy.
Company Profile	Fast growing companies who want to invest in an affordable solution capable of growing with them, as well as the flexibility of anywhere, anytime access without investing in IT infrastructure.	Established companies with the ability to make the required upfront investment to purchase and implement the software. Minimum timeframe for an on-premise solution should be 5 – 7 years.
Remote Locations	Have multiple sites or many geographic locations but do not want to build or support remote access to existing network. May have to comply with unique data residency requirements across a variety of locations.	Have multiple sites across geographic locations and have a supporting network infrastructure.
Initial Services Investment	Implementation services tend to cost less than on-premise solutions since installation, infrastructure preparation, and some configuration are completed by the SaaS vendor.	A good rule of thumb: Expect to spend anywhere from $1-2 for every dollar spent on the initial software license.
Ongoing Services Investment	Business process consulting as necessary.	Software upgrades every 12 – 24 months; technical support and business process consulting as necessary.
Hardware / Infrastructure Investment	A reliable Internet connection.	Traditional IT components including server hardware and software, data backups, storage, disaster recovery, and remote access and network connectivity.
Implementation Time	Implementation time tends to be less than on-premise solutions since installation, infrastructure prep, and some configuration are completed by the SaaS vendor.	Implementation time tends to be a bit longer and more involved. Expect to add 1–2 months to the timeline for a comparable cloud-based implementation.
CapEx vs. OpEx	The subscription model converts traditional technology capital expenses into an operational expense, which can be positive for maximum cash flow flexibility.	Software and hardware are capital expenses.

About Druva

Druva is the leader in converged data protection, bringing data-center class availability and governance to the mobile workforce. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc**.

Q316-CON-10543

druva

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44(0)20.3750.9440
APJ: +919886120215
sales@druva.com
www.druva.com