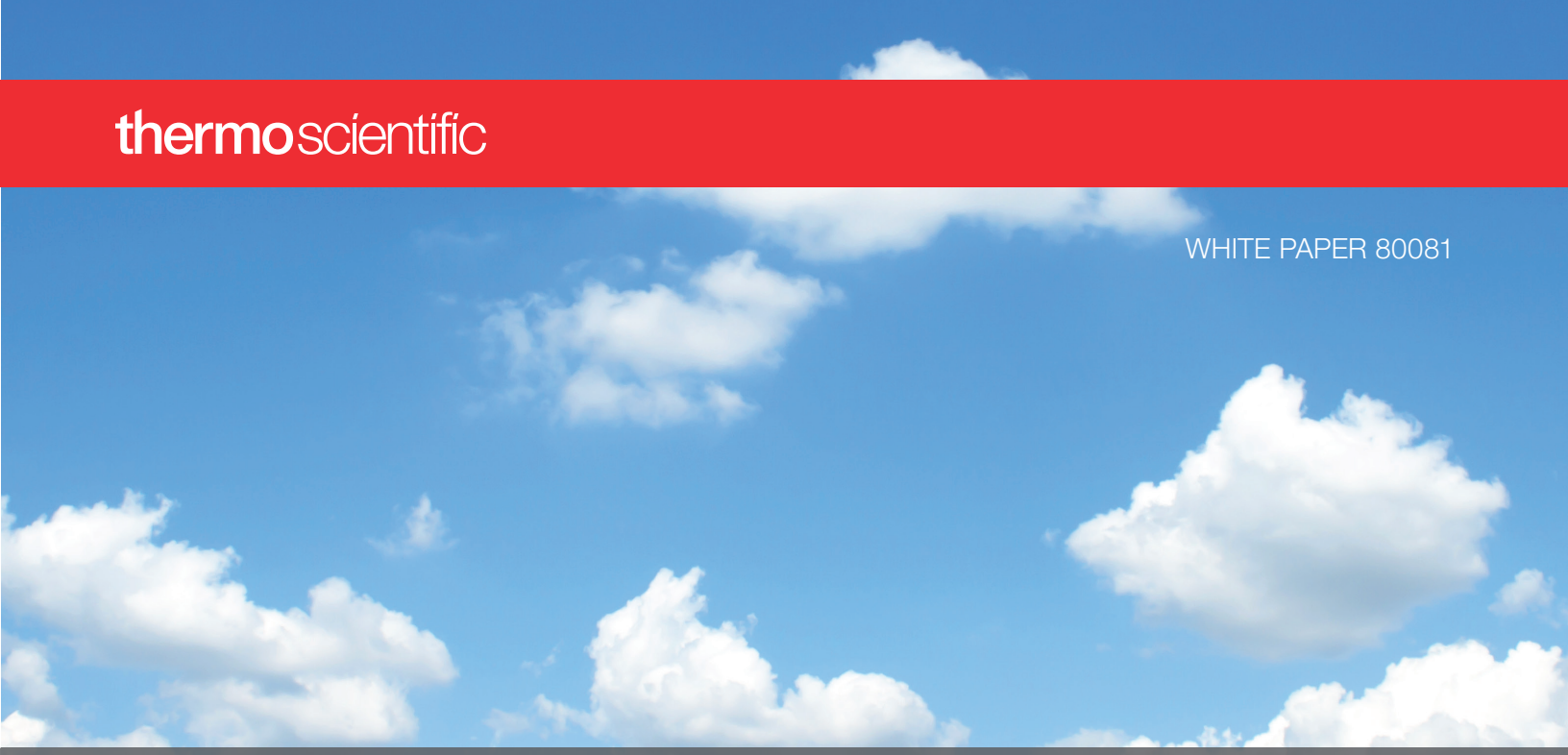
thermo scientific



WHITE PAPER 80081

Integrated Informatics in the Cloud: The Sky's the Limit or Pie in the Sky?

Author

Darren Barrington-Light,
Senior Manager, Product Marketing,
Informatics and Chromatography
Software, Thermo Fisher Scientific

Keywords

Cloud computing, paperless lab, Software as a Service, SaaS, Desktop as a Service, DaaS, Infrastructure as a Service, IaaS, Platform as a Service, PaaS

Summary

With the global proliferation and rapid adoption of cloud computing, laboratories are increasingly looking to take advantage of the benefits of the cloud, especially smaller companies where IT expertise is often lacking. With low entry and on-going maintenance costs, cloud computing represents a cost effective option for these smaller companies to implement enterprise laboratory solutions.

This White Paper will discuss the options available today for laboratory software systems moving from a traditional on-premise setup to a cloud based deployment and the associated benefits and challenges.

ThermoFisher SCIENTIFIC

Introduction

Cloud computing, often referred to as simply “the cloud”, has become ubiquitous in the world around us, powering our day-to-day job responsibilities, enriching our daily lives, and providing computing capabilities far beyond what was imaginable in the late 20th century.

Most of us use the cloud in our daily lives, maybe without even realizing it. Web-based e-mail has become commonplace and most people are happy for their e-mails, photos, and other media to be stored and processed through an unknown server in an unknown location, as long as it’s easily accessible from a web browser or some other internet connected device.

Indeed the number of internet (and hence cloud) connected devices is growing rapidly. The Internet of Things (IoT) refers to the connection of everyday objects to the Internet and to one another, with the goal being to provide users with smarter, more efficient experiences. As a result, huge numbers of consumer devices are now being designed with built-in wireless connectivity, so that they can be monitored, controlled and linked over the Internet via a mobile app. And the IoT is starting to come to the laboratory; devices such as freezers, HVAC (heating, ventilation and air conditioning) systems, thermostats, and other instrumentation can now be connected to the internet for remote monitoring.

All of these IoT devices generate vast amounts of data from diverse locations, with the consequent necessity for quick aggregation of the data, and an increase in the need to index, store, and process the data more effectively. The cloud is the logical solution for handling all this data and delivering the apps for monitoring and control.

But what exactly is the cloud and why are so many businesses looking at it? What are the potential benefits and risks to a laboratory utilizing the cloud to supply software and hardware to manage data and day-to-day operations?

What is the Cloud?

Cloud computing can be defined as: “The delivery of on-demand computing resources – everything from applications to data centers – over the internet, on a pay-for-use basis.”

So instead of the hardware and software sitting on a company’s premises, applications and data are hosted on centralized virtual servers in a cloud data center supplied by another remote company and accessed via an internet connection. The hardware and software are delivered as a service allowing for payment for the resources in small, regular monthly payments and only paying for what is used.

How is the Cloud supplied and utilized?

We have a definition of what cloud computing is but the next question must be how is it delivered or accessed? This is explained in the service and deployment models below which describe the various levels of service provided and how organizations can utilize the cloud.

Service Models

There are three primary service models for cloud computing; Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) as shown in Figure 1. These models offer increasing cloud involvement so they are therefore often portrayed as layers in a stack.

Application	On premise	On premise	On premise	Cloud
App Development, Operating System	On premise	On premise	Cloud	Cloud
Server, Storage, Networking	On premise	Cloud	Cloud	Cloud
	Traditional	**IaaS**	**PaaS**	**SaaS**

Figure 1. Service model comparison of cloud services versus traditional on premise infrastructure

Infrastructure as a Service (IaaS)

This model provides a replacement for the traditional IT hardware infrastructure providing companies with computing resources including servers, networking, storage, and data center space in a wholly managed, pay-per-use manner. The services provided are very comprehensive, scalable and flexible.

Platform as a Service (PaaS)

This level of service provides a platform which allows the development, delivery and management of web-based (cloud) applications without the added complexity of building infrastructure on top of the IaaS layer. The operating systems and network access are not managed by the consumer. This allows application development and deployment to be much faster and more cost effective so Paas is therefore mainly geared toward software development.

Software as a Service (SaaS)

These are complete applications centrally hosted in the cloud and accessed through the internet, usually via a web browser, and normally associated with a periodic subscription. With SaaS, it is no longer necessary to purchase, install, update or maintain the software and associated in-house infrastructure.

Desktop as a Service (DaaS)

A further service model which could be considered part of IaaS is DaaS. In this model a virtual desktop infrastructure (VDI) is delivered as a cloud service with the service provider managing the back-end responsibilities of data storage, backup, security and upgrades. While the provider handles all the back-end infrastructure costs and maintenance, companies usually manage their own desktop images, applications and security, unless those desktop management services are part of the subscription.

Deployment Models

There are also several deployment models depending on your requirements, and the following deployment models have specific characteristics that support the needs of services and users in particular ways (see Figure 2).

Private Cloud

In this model the cloud infrastructure is deployed, maintained and operated specifically for one company. The operation may be entirely on the premises or hosted externally.

Community Cloud

An extension of the private cloud model is a community cloud where a private cloud infrastructure is shared among a number of organizations with similar interests and requirements. Typically these are externally hosted but can be internally hosted by one of the organizations.

Public Cloud

For this model the Cloud infrastructure is made available to the public on a commercial basis by a cloud service provider. This enables the development, deployment and usage of the service in the cloud, with very little financial outlay compared to the capital expenditure requirements normally associated with other deployment options.

Hybrid Cloud

This deployment model's cloud infrastructure consists of a number of clouds of any type, but the clouds have the ability through their interfaces to allow data and/or applications to be moved from one cloud to another. This can be a combination of private and public clouds that supports the retention of some data in an organization, while retaining the ability to use services in the cloud.

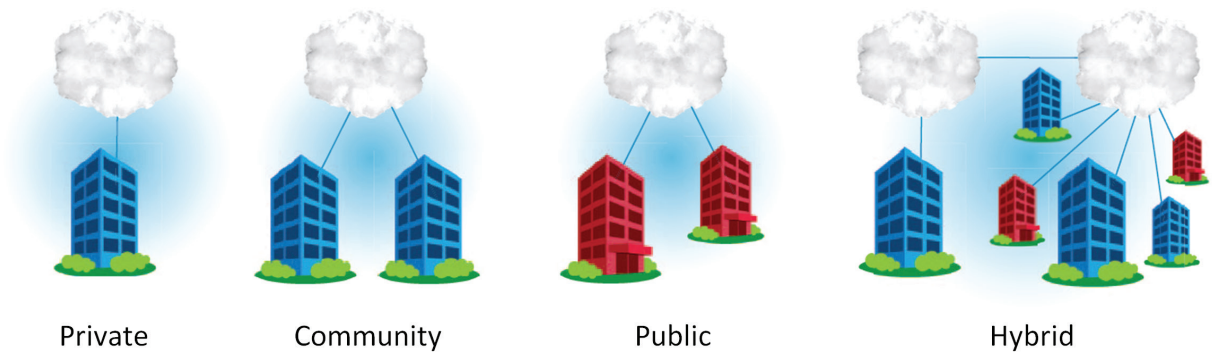


Figure 2. Cloud Deployment Models

Why Move to the Cloud?

There are many benefits for laboratories moving their operations to the cloud including increased efficiency, improved cash flow and many more benefits.

Reduced operating costs

When hosted cloud services replace on-premise IT operations, companies can dramatically reduce their capital expenditure (CapEx) and use operational expenditure (OpEx) for delivering their computing capabilities. And, of course, significant cost savings are achieved (and passed on by cloud services providers) because the cloud IT resources can be securely shared. The result:

- Companies only pay for what they use
- The total cost of ownership (TCO) plunges
- The return on investment (ROI) and time-to-value accelerate

These cost savings significantly lower the barrier to advanced computing resources particularly for small-to-medium businesses where the ROI in the medium to long term will be even greater since upgrades are handled by the provider, negating the need for project teams or consultants, along with the benefit of reducing in-house IT resources for system support.

Flexibility and scalability

Cloud computing makes it easier for companies to scale their services; they can start with an initial deployment and rapidly grow or scale back if necessary. Since the computing resources are managed through software, they can be deployed very quickly as new requirements arise allowing companies to dynamically scale resources up or down at peak or quiet times, enabling them to satisfy consumer demands with minimal interaction. This means the entire IT environment is more responsive and flexible without adding work or cost.

Reliability

With a managed service platform, cloud computing is much more reliable and consistent than in house IT infrastructure. Most cloud providers offer a Service Level Agreement which guarantees 24/7/365 and up to 99.99% availability. Companies can benefit from a massive pool of redundant IT resources, as well as quick failover mechanisms—if a server fails, hosted applications and services can easily be moved to another available server. Also, since all data is stored in the cloud, backing it up and restoring it is much easier. Furthermore, most cloud service providers are usually competent enough to handle recovery of information. This makes the entire process of backup and recovery much simpler than other traditional methods of data storage.

Anywhere, Anytime Collaboration

Cloud ensures data and applications are available to users no matter where they are in the world. Users working off-site can access their work just as easily at home or on the move as they can in the office. They can take their work anywhere via smart phones, tablets or internet-connected laptops without the need to set up a virtual private network (VPN).

Cloud Computing Challenges

Cloud computing represents a big change in how IT does things and, as with any new technology proposition, cloud comes with some concerns. Handing over control to an external entity can sit uncomfortably with some and, while the concerns described below are genuine, the ability to mitigate them means the benefits of cloud generally far outweigh any concerns.

Security

Because cloud computing represents a new computing model, there is a degree of uncertainty about how security at all levels (e.g., network, host, application, and data levels) can be achieved and therefore security is probably the top concern of cloud computing. Placing sensitive information in the infrastructure of a third-party cloud service provider can be a concern for many companies. Being entirely based on the Internet makes the cloud potentially vulnerable to exploitation of loopholes and vulnerabilities within the system which, with important business data being present, could represent a security risk.

Of course, cloud service providers implement and maintain the best security standards and industry certifications to prevent this. The fact that cloud computing is a distributed network also makes it easier for companies to quickly recover from nefarious attacks should they occur.

Privacy

In cloud computing, there is variability in terms of where the data storage, data processing, and data access occurs. Given this variability, different privacy rules and regulations may apply, and when your data is your Intellectual Property (IP), putting that in the hands of a third party could be a risk.

As data in a public cloud could cross international borders, this could lead to different legal requirements around privacy protection of individuals' information and IP; and it is not altogether clear whether cloud computing provides adequate protection, or whether organizations could be found in violation of regulations. As a result, some cloud providers are offering Virtual Private Clouds that allow a business to connect its existing infrastructure to a set of isolated compute resources via a VPN connection and thereby guarantee the location and security of their data within a known legislative area.

Validation

Another concern for risk in cloud environments is computer system validation (CSV) particularly for those working in highly regulated environments, such as those in the pharmaceutical industry. These companies must demonstrate that controls are in place to ensure the computer system, which includes the laboratory software, meets specifications and that it fulfills its intended purpose.

In traditional on-premise systems the company can govern their own systems, control the pace of upgrades and run extensive validation cycles on those upgrades. This conflicts with the cloud delivery model, which favors frequent releases of new features at a pace controlled by the cloud provider.

Some cloud providers are now helping these companies stay compliant by offering 21 CFR Part 11 compliant clouds with a complete set of system documentation that gives full traceability for all changes to the cloud infrastructure alongside procedures and controls designed to ensure the authenticity, integrity, and confidentiality of data.

Reliability

Yes, this is a concern as well as a benefit! Enterprise applications are now so critical that they must be reliable and available to support 24/7/365 operations. Though it is true that information and data on the cloud can be accessed anywhere anytime, even cloud service providers are prone to outages and other technical issues. This could lead to business processes being temporarily suspended although many cloud providers offer a service of at least 99.95% reliability with additional service levels that can guarantee higher availability.

Additionally, if your internet connection is offline, you will not be able to access any of your applications, servers or data in the cloud – this is unlikely to be an issue for many companies but worth remembering.

Control

Since the cloud infrastructure is entirely owned, managed and monitored by the service provider, it gives minimal control to the consumer. They can only operate and manage the applications, data and services sitting on top of the cloud infrastructure, not any key administrative tasks. This is unlikely to be a concern for laboratory systems where typically IT requirements are straightforward.

Integration

It is important to be able to integrate cloud-based applications with on-premise applications that may reside in a private cloud or on traditional technology. A lack of interoperability between these systems can affect the integrity and consistency of a company's data and processes and should be considered in any cloud migration plans.

Cloud Deployment in the Laboratory

The proven cost, performance, and stability advantages of cloud computing significantly outweigh the concerns for most people placing it firmly on the migration path of many private and public laboratories.

With Laboratory Information Management Systems (LIMS), Chromatography Data Systems (CDS), Scientific Data Management Systems (SDMS), and Electronic Laboratory Notebooks (ELN) now commonplace, alongside widespread virtualization of central IT resources, many laboratories are looking to take the next step and harness the power of the cloud to help drive productivity and reduce costs.

However, one of the key characteristics of cloud computing is device and location independence which may not be achievable in laboratories where many legacy instruments often operate on technology which cannot support the cloud and cannot be readily replaced. Also, the quantity of data produced by these instruments may not lend itself to storage and retrieval in a cloud based solution, for example, a high resolution mass spectrometer may produce a file size in excess of one gigabyte; storing and working with this data remotely could introduce significant unworkable delays. Hence the instrument-centric IT infrastructure of laboratories presents challenges that require a combination of laboratory expertise and information technology to successfully complete the migration without disrupting laboratory operations.

IaaS Deployment

IaaS is probably the most common entry point for laboratories to cloud computing. Uplifting all the on-premise backend hardware and software for data storage and management to the cloud delivers many advantages without the need to deal with the instrument issue. Servers and databases can be easily migrated and utilized in the same way as virtualized servers are currently used with the benefits of increased performance and lower cost.

This use of IaaS is particularly suited to laboratory software which has been optimized for operation in virtualized environments and across wide area networks like LIMS, such as Thermo Scientific™ SampleManager™ LIMS, or CDS, such as Thermo Scientific™ Chromeleon™ CDS software. Of course not all laboratory software systems will have been optimized and therefore these may not be suitable for cloud deployment; hence care must be taken over product selection if operating in the cloud is either desired or required.

For optimized systems, the central resources can be easily moved to the cloud, for example, a cloud-based Chromeleon DataVault would see the database and raw data storage moved to the cloud (see Figure 3) while maintaining on-premise instrument PC's for data collection thus ensuring continuity within the lab and alleviating the need to send data directly to the cloud from an instrument.

Of course in modern CDS software it is now also common to virtualize the CDS client application using terminal server–style application publication (also known as server-based computing), in which applications run on a terminal server with output sent to users' computers. These computers rely on the server to operate providing only display, keyboard, mouse and basic processing power in order to interact with the server. They do not store any data locally and are very thin in features and functionality – hence they are known as 'thin clients'. The overhead costs associated with administration, maintenance, support, security and installation of these thin clients are significantly lower than a traditional PC.

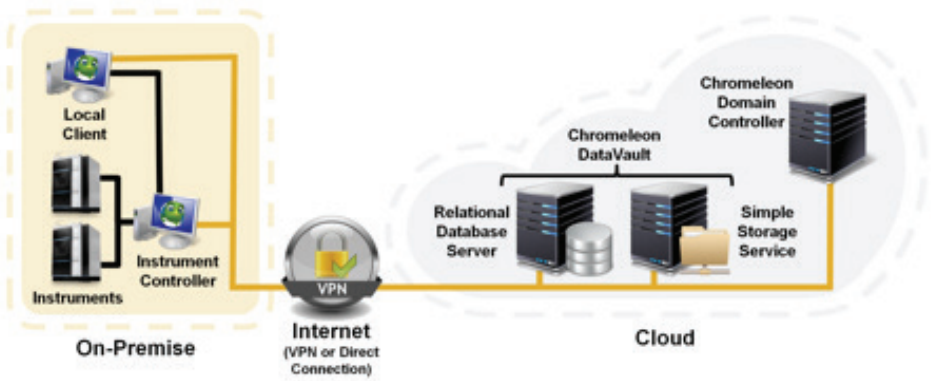


Figure 3. Chromeleon CDS Cloud Deployment Example

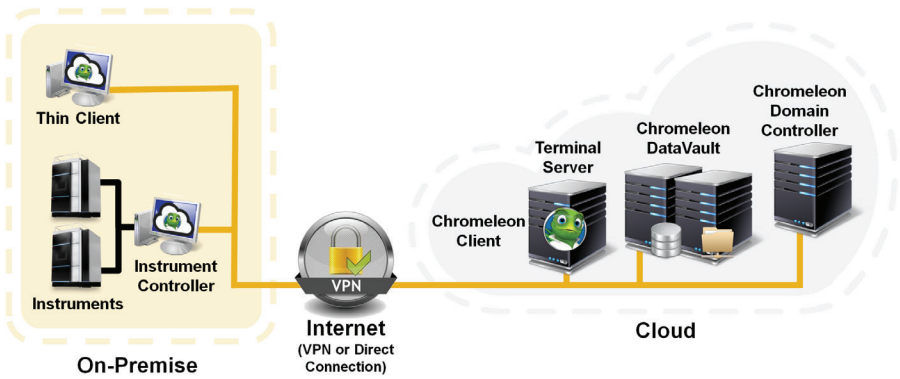


Figure 4. Chromeleon CDS Thin Client Cloud Deployment Example

Thin clients can be easily supported by a cloud deployment as demonstrated in Figure 4, further reducing the on-premise infrastructure, simplifying implementation, reducing validation, and boosting application performance by utilizing the computing power of the cloud.

Software systems which don't necessarily need resources installed locally or provide web or mobile clients, such as SampleManager LIMS, also lend themselves very well to IaaS cloud deployment as they can support operation via a standard web browser reducing or even removing the need for dedicated application software in the laboratory delivering cost, performance, security and stability benefits (see Figure 5). SampleManager LIMS also provides functionality that enables integration to laboratory instruments from the cloud. This allows automatic result entry, preventing manual data entry errors and reducing data integrity and compliance risks.

Indeed many Thermo Fisher Scientific customers are using the cloud to host back end services for both Chromeleon CDS and SampleManager LIMS. They have successfully tested and deployed enterprise systems using Amazon™ Web Services™ (AWS), Microsoft™ Azure™ and other cloud providers and in the process delivered improved performance and cost reductions.

Hybrid Cloud Deployment

Of course with laboratory software systems being so critical to daily operations the concern of losing connection to the cloud remains. Data loss is unacceptable and having a laboratory unable to function due to an outage is not an option. For this reason some companies may look to use hybrid clouds – part private and part public – to offset this risk (see Figure 6).

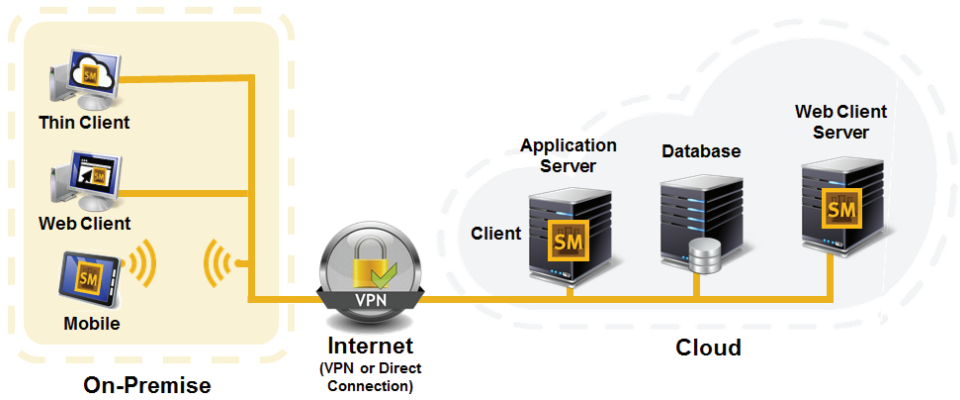


Figure 5. SampleManager LIMS Cloud Deployment Example

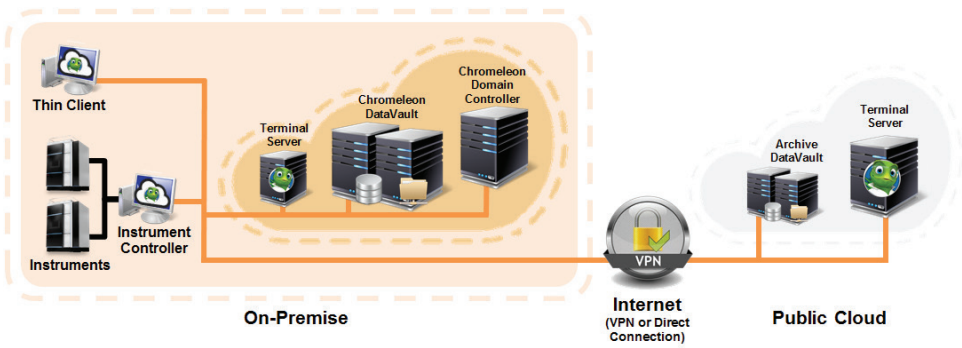


Figure 6. Chromeleon CDS Hybrid Cloud Deployment Example

In this scenario, a private cloud could host the data and associated servers, giving total control over security and uptime, while leveraging the computing power of a public cloud to provide on-demand elasticity for client operations in peak periods. The public cloud could also be used for archiving and disaster recovery of the private cloud data and, should the public cloud become unavailable, the private one can maintain laboratory operations.

This hybrid approach can provide a secure solution for companies who have the capability to create and host their own private cloud but for many smaller companies this may not be feasible.

Product Licensing in the Cloud

Of course with the ability to effectively rent the infrastructure for your laboratory software comes the question of renting the actual software itself, be it LIMS, CDS, SDMS, ELN or something else. Could these software licenses be provided on demand with only consumed licenses being paid for? This could again offer cost savings to companies but also offer flexibility for scale up and down that has never previously been possible.

Well, SampleManager already offers the ability to rent licenses rather than purchase outright, which could be the first step towards an on-demand licensing system, although that may still be some time in the future.

Thermo Fisher Cloud

And talking of the future, what about the possibility of lab software vendors providing a hosted SaaS solution for laboratory software?

Well, steps are already being taken in this direction. For example, Thermo Fisher Scientific has it's own cloud – the Thermo Fisher Cloud – which has been built on the AWS platform using a virtual private cloud securely partitioning it from any public access.

One of the platforms it hosts is Thermo Fisher Connect, an ecosystem of scientific analysis, remote instrument access, data storage and collaboration tools. It offers several SaaS applications including AppConnect, a range of web-based applications for analysis of large data sets, Instrument Connect, a remote monitoring app to stay connected to Thermo Fisher cloud-enabled instruments, and Cloud Connect Utility that facilitates data storage and sharing for any instrument connected to an internet enabled PC. These kinds of applications could be the first steps towards cloud deployment of laboratory software systems.

Conclusion

With the global proliferation and rapid adoption of cloud computing, laboratories are increasingly looking to take advantage of the benefits of cloud, especially smaller companies where IT expertise is often lacking. With low entry and on-going maintenance costs, cloud computing represents a cost effective option for these smaller companies to implement enterprise laboratory solutions.

With modern CDS and LIMS software, such as Chromeleon and SampleManager, lending themselves well to IaaS deployment, all companies can now harness the increased security, improved performance and cost savings delivered by the cloud.

Interested in our complete data management solution?
Learn more about the entire Thermo Scientific Integrated Informatics portfolio at **thermofisher.com/integratedinformatics**

Like Charlie Chromeleon on Facebook to follow his travels and get important updates on chromatography software!
facebook.com/CharlieLovesChromatography

Visit AppsLab Library for online access to applications for GC, IC, LC, MS and more. **thermofisher.com/AppsLab**

Find out more at **thermofisher.com/integratedinformatics**

ThermoFisher SCIENTIFIC