

CHOOSING A SECURE PRIVATE CLOUD PLATFORM



- 01 Introduction
- 02 Understanding the Benefits
- 03 Setting Selection Criteria
- 04 In Closing
- 05 About the Author
- 06 About Mycroft Inc.



At first glance, the goal of cutting costs while continually increasing efficiency and flexibility seems contradictory and certainly daunting. It is specifically with this challenge in mind that the following guide was created to introduce concepts, strategies and a simple formula for selecting a secure cloud platform for application deployments that makes sense - not only for reaching company goals, but also one built for the future.

As each reader makes this journey, new strategies and directions will come clear and beckon the needed step forward.

Let's get started.

~ Jonathan Freeman

Founder, Mycroft Inc.

Private Cloud Environments = Cost Effective & Secure

Before diving into the details, four critical points need to jump out at each and every reader as options for selecting a secure cloud platform for application deployments are evaluated.

Private cloud platforms - in the very nature of how the technology evolved - has proven to be **QUICK** and **COST EFFECTIVE** to implement and leads to some of the most **SECURE**, streamlined environments available today.

Increasingly, organizations are moving away from the traditional wholly owned & operated data center model of the past four decades. Underutilized assets, overburdened facilities, reduced resources & rising energy costs are fueling a growing disdain for building, managing & maintaining on-site data centers. The combination is sending companies searching for a lightweight option that is both affordable and efficient.

With that said, for some the very idea of the cloud attaches a certain sense of mistrust about security, stemming most recently from breaches reported by Amazon, Sony, RSA and others.

But just for a moment before we move through the distinct differences between public and enterprise private clouds, clear out that misconception and remember this:

Enterprise private cloud adoption has been proven to...

- Reduce CAPEX costs
- Decrease time-to-market
- Boost scalability
- Accelerate deployment time
- Provides high level of security

As cloud industry growth shows - 45% of large enterprises adopted a cloud model in 2010 vs. 28% in 2009 - there can be a variety of scenarios for placement, but if its security you seek to guarantee, enterprise private clouds are leading the way.

Take a look at the pros and cons of both and keep in mind your application deployment needs as we begin to dig deeper.

Private Cloud

- More expensive to deploy
- Highest level of control, compliance & security (data loss, hacking etc)
- Knowledge of where assets are located
- Highest assurance level for guaranteed availability & consistency
- Fully managed, support models available through complex service providers
- Authentication, authorization, provisioning, role management, GRC, audit & logging can sit behind firewall
- Cost savings through eliminating company-owned and operated data center
- Reduced internal IT staffing needs
- Self-service option available

**Public Cloud**

- Cheaper to maintain & deploy
- Lower control level with shared servers; where assets are located
- Lower security levels to protect against hacking, data loss, traffic spikes (i.e. Amazon, Sony)
- Offers flexibility to quickly expand
- Lower assurance level for availability & consistency
- Cost savings through eliminating company-owned and operated data center
- Reduced internal IT staffing needs

Now that we've defined public & private cloud differences, let's nail down what your secure cloud platform needs to deliver.

It comes down to the basics:

- Reducing risk by moving management of complex processes
- Easily adding functionality as you need it
- Guaranteeing scalability & elasticity
- Decreasing acquisition & implementation costs
- Driving higher efficiencies in solution deployment times
- Establishing competitive advantage & future-proof strategies
- Reduce costs through increased utilization of idle assets



Establishing strong selection criteria for evaluating private cloud platforms needs to focus on specific differentiators. Asking the right questions is critical in extracting the information that will directly lead to the successful adoption of the right solution. Leveraging an easy-to-implement questionnaire will yield a quick and efficient evaluation to focus the selection process.

The Service Provider Questionnaire will establish two important insights - first, an understanding of the **key services and expertise** available and second, the level of **scalability and flexibility**.

Take a look at an example of an effective questionnaire - one specifically designed to clarify the needed service offering components for the right path forward.



The Service Provider Questionnaire

- 1 Is a subscription model offered?
- 2 Is there a choice of hosted or on-premise?
- 3 How long is the implementation process?
- 4 Does the platform come wrapped with a fully managed service?
 - If so, how many levels of support are there?
 - Is there 24/7 support & customer help desk option?
- 5 Does the platform allow for unplanned usage spikes & dips?
- 6 Does the solution feature a self-service portal option?
- 7 Does the platform feature industry-proven identity and security best practices in an encapsulated, subscription-based solution?
- 8 If so, is there a full set of security product offerings including identity & data management, controls & attestation and compliance?
- 9 Does the provider have a professional security consulting service?
- 10 Does the provider offer a guaranteed SLA?

If you weren't looking for cost-savings and a **higher level of availability & consistency**, you wouldn't be looking at all. Finding it comes down to one critical statement - the right platform must deliver a viable alternative to multi-tenant, public clouds with the intrinsic capability to **Build Once, Deploy Often**.

It may seem like a simple statement, but holds the key to acquiring a platform that can grow with your enterprise without the pain of expensive and time consuming reconfigurations and deployments.

So what does Build Once, Deploy Often really mean you may wonder? Let's find out.

Defining Build Once, Deploy Often

Build Once, Deploy Often can be likened to the same concept that made franchising so successful. Once a base template has been built based on proven best practices, it is deployed in the same way with the same attributes across the board. Think of any one of the staple fast food chains, order a hamburger in Hong Kong, New York City or Sydney Australia and each time you can expect the same level of consistency and repeatability. In the world of secure application deployments, the same holds true.

Take a look at the critical components of a Build Once, Deploy Often model and work it into your vendor evaluation plan.

- Solutions constructed from common set of security instrumented appliances that are pre-integrated into a security operations center for monitoring & management
- Full encapsulation of network & server infrastructure
- Consistent, secure solutions that are portable across any service provider
- Provides full instrumentation & securitization
- Creates foundation for freedom of choice — deployments can be mixture of internal private data centers, contracted co-location data centers & public cloud providers

Remember... Repeatable & Scalable

Hold on, you're almost there...

Remember one concept above all else: Your new secure private cloud platform - from its foundation up - must be built for the future. What that means is simple, whichever solution you choose needs to be repeatable and scalable. Equally as important is the level of expertise and management of the service provider. The combination of seamlessly integrated best practices and management with a repeatable and scalable platform will not only yield 100% peace-of-mind that your applications are secure, but also a future proof path for continued cost savings and efficiency.



You did it. You're ready to make a move!

All your information is gathered, your evaluation is complete and the right secure private cloud partner has come clear.

Be bold, champion what you've learned across the company and focus on building the motivation to move through the decision process swiftly and with purpose.

The benefits are there for the reaping - now and all along your future growth path.

All you have to do now is grab it.



MAKE A MOVE.

BE BOLD.

BUILD MOTIVATION.

CHAMPION WHAT YOU'VE LEARNED.

05

About the Author



Jonathan Freeman is the Founder and Chief Information Officer for Mycroft Inc. In this role, he is responsible for research and development of the company's marketing-leading innovations that deliver security solutions to the enterprise private cloud. Freeman has more than 20 years of experience in successfully developing, commercializing and growing breakthrough identity and access management technologies. As an early advocate of directory-based architectures and virtual communities, Freeman has delivered next generation solutions that leverage his software heritage and knowledge of customer needs. Freeman is a recognized visionary in the development and deployment of Security as a Service and Enterprise Private Cloud solutions and works with strategic partners and customers to deliver business-focused solutions in the Identity Management, Security and Managed Service Provider markets. Freeman founded Mycroft Inc. in 1988 and holds a Bachelors of Science degree from Columbia University.

06

About Mycroft Inc.



Mycroft Inc. is the innovation leader in delivering cloud-based IT identity and security solutions as a service. Focused on the configuration, delivery and management of its offerings, the company seamlessly integrates software and professional services expertise to provide enterprise implementations and a portable fully managed private cloud-based offering.

Mycroft Inc. is headquartered in New York City and St. Louis with service centers in the UK, Ireland and India. For more information, visit www.mycroftinc.com or call 212-983-2656 ext. 1.