



# Cloud security, options and trends

**Shahin Pirooz, Chief Technology and Security Officer and Executive Vice-President of cloud solutions provider Center-Beam, Inc.** offers his expert analysis of the nature of security in the cloud environment, and how to tailor your cloud infrastructure to meet your organization's needs.

To listen to this podcast visit: <http://www.globaletm.com>



**David: Shahin, give us a brief overview of CenterBeam.**

**Shahin:** CenterBeam was founded in 1999 with the concept of delivering enterprise 100 class services to the mid-market. We were the first Software-as-a Service [SaaS] company to deliver multi-tenant Exchange as one of our core foundation services, also providing remote management capabilities to mid-market enterprises. Over the last 10 years, we have developed a lot of experience and gained traction in delivering not only SaaS, but also cloud capabilities to allow customers to virtualize their environment and move their physical equipment out of their infrastructure to a virtual cloud-based data center.

**David: One of today's hot topics is security. As Chief Security Officer, what do you see as the most important considerations when it comes to security, especially concerning the cloud?**

**Shahin:** I think that security is one of the most misused and misunderstood terms in the market, and, specifically, as it relates to the cloud. A lot of the fear and uncertainty is being fueled by the media. While there are valid questions about “will my data be safe in the cloud”, and whether I trust it in somebody else’s data center, I think the underlying concern is that people don’t know what to ask or what to focus their questions on when speaking to a cloud provider. For example, being secure as opposed to what, is a question that comes to my mind. If you look at existing environments today in the mid-market, not a lot of time and money is spent on securing infrastructure. Heightening the concern that cloud environments are less secure than local infrastructure is the media, in the way they cover breaches and issues that have occurred.

The reality is the security mishaps that we see in the market and covered in the media are largely a result of poor development - by developers that integrate between the cloud and the internal environment, creating holes in the applications they write, these holes are then used to compromise data. Or there is a set of open APIs [application programming interfaces] that the cloud

provider provides that can be used equally by hackers as well as the developers that are trying to integrate into the system.

My recommendation to clients and prospects is the criticality of approaching security in the cloud just as you would in your own data center. You should have firewalls before and after your DMZ [demilitarized zone] environment, and not allow direct access to your core infrastructure. And follow the best practices that you would if you were building your own data center. Don’t change the way you operate, despite the experiences and lessons you have learned over the years as an IT expert, simply because the solution is in a cloud rather than in your data center.

**David: We are also hearing a lot about virtual data centers. Could you tell us more about it and how it is different from cloud computing?**

**Shahin:** The word ‘cloud’ is very generic and covers a wide range of services and capabilities. Virtual data centers are simply another way of delivering cloud services. At its core, the virtual data center takes what customers would typically call their co-location facilities, and moves it into a cloud provider’s infrastructure and delivers it as a virtual infrastructure versus a physical infrastructure. With a virtual data center, the co-location facility is all virtual, and it is hosted in a provider’s infrastructure rather than having to build all aspects of it.

A lot of providers out there call themselves cloud providers, yet they are really only delivering Infrastructure as a Service [IaaS]. The easiest distinction is a IaaS provider leaves service integration to you. This means if you have a multi-tier application, you have to build each of those tiers in that IaaS platform by yourself. If you have a web front end, you have to configure the web server. You may also have to configure the database server and, on an application front for the client’s side, you would have to build your terminal services or Citrix environment to deliver that client application.

What we have done is different. We have taken a mix of infrastructure and platforms, comprised of both web and database hosting, to create a service that delivers all four tiers in a pre-designed, pre-built solution that is tightly integrated.

This allows a customer to take advantage of the pieces and parts that fulfill the tiers needed to deliver their application. In the process, what we have done is created the ability to take a non-SaaS application, one that typically isn’t designed to be delivered via the cloud, and with the combination of our four-tier architecture and the virtual data center, made it SaaS-able.

**David: What is your opinion on Hybrid Cloud?**

**Shahin:** I feel, without exception, that a hybrid cloud is the only way to go. Why? It is because most organizations benefit from a phased approach to entering the cloud, and the hybrid model offers a way to leverage the advantages of the cloud without disrupting your current business processes and requirements. Hybrid clouds are no more than an integrated system of services, some that reside within your facilities or co-location environments, and some within a cloud provider. There are some workloads that are not yet fully capable of being moved into the cloud unless you move the entire application eco-system to the cloud. For some customers it isn’t practical either because they can’t afford to, or they have a significant capital investment sunk into their existing environment making it unviable to pick up everything and move it into the cloud. So the hybrid cloud enables the customer to move at their own pace as opposed to a pace of the provider. We embrace the hybrid cloud, and we encourage our customers to do so as well.

**David: The IT landscape is constantly changing, but looking forward what do you see as the biggest game changers today in cloud infrastructure?**

**Shahin:** If you are paying any attention to the media, there are a lot of advertising and PR dollars being thrown around by giants like Microsoft and Google, trying to depict collaboration as the next big thing everyone will move to adopt. The reality is we released multi-tenant Exchange over a decade ago, and collaboration is not new to the market space. It is something that will continue to evolve, and we will see more and more capabilities added to it. If I were to

focus in on trends specific to the cloud environment, I see customers focusing on two things. The first being they don't want to refresh their hardware anymore. They are tired of the four or five-year cycles that require them to constantly rebuild and manage their infrastructure. By moving to a virtual workload model, both in a hybrid and a cloud-hosted model, they are able to eliminate the concept of a hardware refresh.

The second area, I think, is emerging from customers' dissatisfaction at having to modify their business and/or security processes to fit a particular cloud or SaaS providers' requirements. The applications that have traditionally been put into a cloud or SaaS environment have been restricted by the ISP [Internet Service Provider], so that you get less functionality than what you are used to in your local environment.

Our approach from the beginning has been to enable as much customization as possible in the cloud environment. This allows the customer to retain their policies rather than CenterBeam forcing our policies onto the customer. This is important because business processes should be the driving forces in terms of

what partners and technologies to pick, and the applications should be picked to align with their business strategies and policies, not selecting a partner and then modifying your processes to fit to those of the partner. This was the norm prior to the cloud and SaaS – and I see customers pushing back on cloud vendors more and more, expecting a level of flexibility to accommodate the customer's business priorities.

In summary, the trend that I see coming is less and less infrastructure in the customer environment, but to be worthy of consideration, cloud providers are going to have to shift their thinking to enable more flexibility and security so that the customer can bring their policies and procedures and apply them to the cloud environment, not the reverse.

**David:** You point out the advantages of the cloud for somebody looking to move into the cloud. What words of advice do you have for them?

**Shahin:** We have discussed selecting the right partner - one who has the scope and breadth of capabilities that allow you to move additional workloads

beyond single point solutions into the environment. However, my underlying message as organizations are thinking of moving more and more workloads to the cloud is you have got to pick a partner that has solid integration experience, not just somebody who says, 'here are the keys, go ahead and fill your boots'. You need somebody that can offer live support so you are not relying on wikis and forums for answers when you run into problems. You also need someone with a breadth of services, so after you deploy the point solution you are working on today and you think about additional workloads you want to move to the cloud, you don't have to pick multiple providers. You can pick a provider that will grow and scale with you. And lastly, you want a degree of flexibility that enables you to do what you do today but in the cloud, and also allows you to modify what you do tomorrow and the platform will support you.

Picking someone who can grow and scale with you, and does not constrain or force you to do things that modify your business processes is probably the most important message for anybody looking to move to the cloud. ■



Shahin Pirooz brings deep experience in strategic IT leadership, including security deployment and operations management. He offers deep technology expertise covering areas such as IT architecture, Cloud/SaaS, Distributed Computing, core tools and Operating Systems.

In his primary role as Chief Security Officer he is responsible for the development, implementation and management of the company's corporate security vision, strategy and programs. He directs staff in identifying, implementing and maintaining security processes across the organization to reduce risk and respond to incidents among others related to data security.

**Shahin Pirooz** |  
EXECUTIVE VICE PRESIDENT, CHIEF  
SECURITY & TECHNOLOGY OFFICER  
CENTERBEAM, INC.