



“Use a critical eye when making decisions of what applications or functions you move to the cloud, and determine what levels of security are required for each.”

*- Shahin Pirooz
CTO, CenterBeam Inc.*

Cloud Security Precautions

EXECUTIVE BRIEF

The Best Defense is a Good Offense

As mid-sized businesses look to the cloud for its dramatic business results—significant CAPEX savings, scalability and the ability to focus IT spending towards projects that contribute to the bottom line—many put on the breaks over security concerns. This doesn't have to be the case for those IT leaders who are clear on their priorities and firm on their requirements. We offer four basic precautions that make a transition to the cloud not only a smart but a safe decision.

4 Practical Precautions

1. First and foremost, don't entrust your security to someone who does not have a track record for delivering secure cloud services.
 - a. Do your homework: has the provider built in redundancies? Where and how? Are their controls around security procedure and practice, IT policies, and infrastructure audited to ensure compliance with the strictest standards and best practices?
 - b. Check their history: have there been security breaches in the past? To what extent? What were the implications to their customers? If there have been past issues, were they remediated?
2. Use a critical eye when making decisions of what applications or functions you move to the cloud, and what levels of security are required for each. When building out your cloud environment, hold your provider(s) to the same security standards you would use if you were deploying it in your own datacenter. Importantly:
 - a. Does the provider you are working with have integration experience? This can be a critical component of ensuring your cloud services operate seamlessly and securely with each other and across your enterprise.
 - b. Never allow direct access to your core. Institute a true tiered network architecture, separating the DMZ from your core network.
 - c. Never deploy a cloud solution without firewalls. You wouldn't do it in your datacenter, so don't do it with a cloud provider. This protects your core network from the public internet to prevent unwanted access to your infrastructure.
 - d. Never deploy a solution that requires you to administer your services over the public internet. Make sure you have VPN connectivity into the cloud provider, making it a secure network. You can then be more comfortable that your cloud services are operating as an extension of your network vs. on servers floating in the cloud somewhere.

3. Make sure your business objectives drive your technology decisions and not vice versa.
 - a. Don't cut corners or make tradeoffs that will put critical areas of your business at risk. This applies whether your infrastructure resides on premise or in the cloud. The cloud is neither more nor less secure than on-premise data storage solutions—it's all a matter of understanding what controls are available.
4. Have a plan in place for failure.
 - a. Just because something moves to the cloud doesn't mean the technology can't fail, or a human won't make an error.
 - b. As you would with other technology aspects, make sure you (and your provider) have a plan for failure, one you are comfortable with and one both of you can execute.

Making a decision to have an expert provider manage your data doesn't mean you should let your guard down. The best offense for smart IT leaders is to implement a strong defense—taking measures to reduce the risks and ensure a secure cloud environment.

About Shahin Pirooz

Mr. Pirooz has been at the forefront of cloud technology for more than a decade. Throughout the evolution from ASP to managed services to what is now commonly known as cloud computing, Pirooz has held critical leadership roles within organizations such as EDS, serving clients including Palm, Philips, VLSI, and Netigy. Pirooz also led development for an early-stage Oracle ASP. As CenterBeam's CTO, his focus has been building CenterBeam's managed service organization to deliver enterprise class IT services to the mid-market. The role extends beyond the responsibility of implementing best practices within CenterBeam—Pirooz is accountable for CenterBeam's customers as well. In essence, Pirooz is an acting chief security officer (CSO) for CenterBeam's customers, providing strategic insight for their security practices.

About CenterBeam

CenterBeam is an IT veteran, with an eleven year track record of delivering secure cloud-based IT services. CenterBeam differentiates itself through its broad service portfolio, providing a cohesive IT solution—independent of where end users are located, what time it is, or whether they're on a Mac®, PC or mobile device. And CenterBeam's Professional Services consultants are available to handle special projects end-to-end or serve as an extension of your in-house team.

