

# CLOUD SECURITY

## CloudDocs: Completing the Document Process

[www.egisticsinc.com/clouddocs](http://www.egisticsinc.com/clouddocs)

Security is paramount in any business, and in any system architecture. Does it make any difference if the system architecture uses cloud services or is strictly in-house? Well, yes and no.



# Some Think Cloud Security Superior to In-house Data Centers

By Randy Davis, VP eGistics



For some in-house data centers, the data security horse has already left the barn

Recently a panel discussion Webinar titled, "Ready for Cloud Storage? Key Considerations and Lessons Learned," was hosted by SNIA, Cloud Storage Initiative.

The panel included Kipp Bertke, Manager of Infrastructure & Operations at Ohio Department of Developmental Disabilities; Ajay Chandramouly, Cloud & Data Center Industry Engagement Manager at Intel; and Nathan McBride, Executive Director of IT at AMAG Pharmaceuticals.

The discussion was meaty and substantial, but the comments by McBride were downright breathtaking. I would say that he and I had been reading the same articles, but his comments were based on hard-earned experience rather than ivory-tower theorizing.

I was so impressed with his views that I am going to quote him as best I can, and quite extensively, in this article.

The following comments from McBride are in response to my question, "Are cloud security concerns qualitatively different than those for on-premise solutions?" Although the question was misinterpreted to mean security differences between public and private clouds, rather than between cloud solutions and in-house (non-cloud) solutions, McBride's answer was spot on.

"Security is always a concern of mine. It brings me to questions I have to ask myself, and they are 'What is the best possible data center I could build? What's the most amount of security I could put into it, and how much would that cost me?' I realized that the cloud storage vendors I selected had spent five times that much, or a hundred times that much, to build their data center. So there's nothing I can do that would even come close to the security offered by my vendor for a low service cost."

Then he addresses the trust issue head on. Can you trust cloud storage service providers?

"People say, 'Well, what about the people at the data center that is hosting your data? Do you trust them?' Well, I trust them just as much as I trust my own IT employees. The only way you can ever be secure is to remove people. Since I can't remove people

from the equation, I have to trust that at a certain level the companies I want to do business with want to keep doing business with their customers, so they're going to employ best methods, best practices, and the best people to manage my data. And I don't just trust that. I also verify through SAS70 certifications, on site audits, things like that. But I do feel comfortable and secure knowing that the companies we are doing business with have employed security practices that far exceed anything I could manage to put together."

McBride went on to discuss some of the data leaks common to in-house data centers, things like non-secured flash drives, data that is copied to dozens or hundreds of PC hard drives, data sent to casual, personally controlled file storage services such as Sky Drive and Google Docs, and so on. His point is that you have to consider the real risks, costs and vulnerabilities of in-house data center management, and realize that, for most companies, it's no Fort Knox for data. On the other hand some cloud storage service providers have gotten real close to Fort Knox-like security.

## **The eGistics "T4" Approach**

eGistics knows that security is your main concern when putting documents in the cloud, but on-line document management doesn't mean you have to compromise on security. In fact, with eGistics, your document management and storage security may actually - and significantly - *improve*.

### **Overview**

We have provided secure storage for America's leading financial institutions for over 15 years, and have continuously increased the levels of security that protect your data -- and make sure only you can get to it. Our on-line document management security environment is being tested and proved by the most punctilious financial institutions in the world.

CloudDocs provides world-class physical and cyber security. Our sites are PCI certified, and SAS 70 I & II, SOC 1 & 2, FFIEC and HIPAA compliant. What's that mean? Well it means that we have the safeguards in place to store very sensitive information. We utilize multiple encryption technologies and best-in-class network intrusion detection. We also provide industry-leading user administration and audit reporting, with customer-administered group and sub-group privileges and audit reporting on all activity.

Our infrastructure includes mirrored, geographically dispersed data centers for real-time business continuity and automatic fail-over. You can be confident that your documents will be available when you need them.

### **User Security**

Only those you give access to can sign on to CloudDocs. Users access the system through a secure Web browser. Login information is protected using 256-bit encryption over SSL.

You can also limit user privileges according to a group or roles.

## Document Transfer

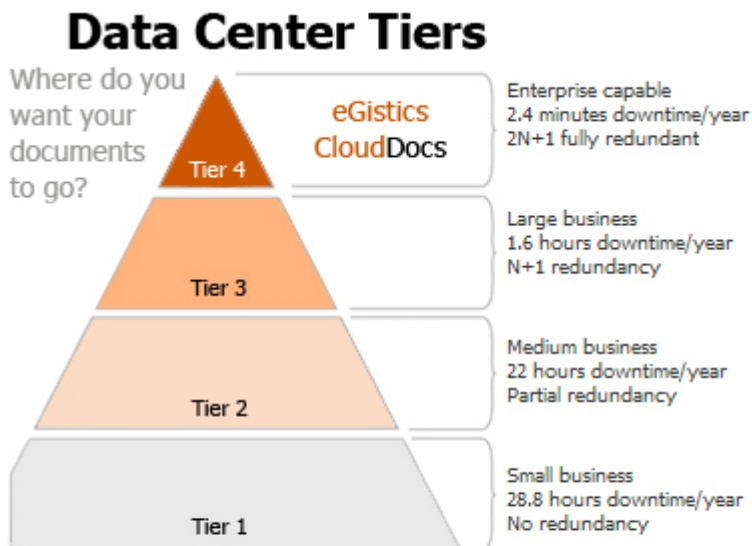
CloudDocs protects your data along the entire document transfer process. We make sure your documents are encrypted as soon as you press the Send button. And we use Secure FTP to transmit them to our digital storage facilities.

## Data Storage

You probably want to know, "Where are my documents stored?" Well, they are stored in world-class data centers with **Tier 4 rating**, meaning that the centers have a fault-tolerant infrastructure, and have met the highest level of security designation possible for data centers.

Here's what you get:

- Redundant communication delivery paths
- Site availability of 99.995%
- Redundant power, cooling, hardware
- Fault tolerance



On top of that CloudDocs on-line document management provides layers of cyber security that protect you (and us) from network intrusions, unauthorized access, viruses, denial of service attacks, and so on.

**Our Commitment to You**  
eGistics holds itself to a high level of service. Please take time to read our Service Level Agreement, and be confident that, no matter what happens to us, your e-documents will be safe and accessible

You have a choice where your valuable business documents are stored. You don't have to settle for anything less than the most secure data centers. Consider the alternatives, and then choose **Tier 4**.

Do you have security concerns about solution providers who use cloud services? Let us know so that we can show you the kind of security that we provide to the top financial services and payments companies in the U.S. They are impressed. We think you will be, too.

---

eGistics does not employ "black cloud" services which store customer data in unknown locations. We, and our partner AT&T, always know where our customers' data is, and we maintain full responsibility for securing and protecting it. We annually pass extremely stringent security audits and reviews by top financial services customers.