**Startup Failure Post-Mortems 2014 Second Update (9/24/2014)**

### Nirvanix

Title: [A Nirvanix Postmortem – Why There’s No Replacement For Due Diligence](http://www.forbes.com/sites/benkepes/2013/09/28/a-nirvanix-post-mortem-why-theres-no-replacement-for-due-diligence/)  
Title Link: <https://www.forbes.com/sites/benkepes/2013/09/28/a-nirvanix-post-mortem-why-theres-no-replacement-for-due-diligence/?sh=79d18d612556>

Product: [Nirvanix](https://www.cbinsights.com/company/nirvanix)  
Product Link: <https://www.cbinsights.com/company/nirvanix>

The cloud is great. Outsourcing is great. Unreliable services aren’t. The bottom line is that no one cares about your data more than you do – there is no replacement for a robust due diligence process and robust thought about avoiding reliance on any one vendor.

# Nirvanix

INTERNET | Internet Software & Services / Data Storage  
[nirvanix.com](https://nirvanix.com/)

## See what CB Insights has to offer

## Founded Year

1998

## Stage

Dead | Dead

## Total Raised

$70M

## About Nirvanix

Nirvanix is a provider of enterprise-class cloud storage services designed specifically for customers with expectations of extreme security, reliability and redundancy. Under its CloudComplete portfolio, Nirvanix offers fully managed public, hybrid and private cloud storage services with usage-based pricing. The company's second generation technology is utilized by IT OEMs and is fully integrated with third-party backup and archiving software products and appliances, enabling One Click to the Cloud.In September 2013, Nirvanix shut down notifiying users they needed to migrate their data

## Nirvanix Headquarter Location

9191 Towne Centre Drive Suite 510

San Diego, California, 92122,

United States

619-764-5650

# A Nirvanix Post Mortem - Why There's No Replacement For Due Diligence

By Ben Kepes Former Contributor Sep 28, 2013,05:40am

Title Link: <https://www.forbes.com/sites/benkepes/2013/09/28/a-nirvanix-post-mortem-why-theres-no-replacement-for-due-diligence/?sh=79d18d612556>

A couple of weeks ago the industry was stunned when cloud storage provider Nirvanix sent an email customers advising them that the company would be shutting down in a fortnight - while the consumer space is used to services coming and going, this was an unreservedly enterprise-grade service - and one that had raised $70M in venture funding to boot. Not only were customers told that the company was shutting down, but they also had to find alternative providers in very short order.

As is often the case in situations like this, there were plaintive wails from the naysayers that this is an example of why cloud computing can't be trusted and why we should all move back to the days of old. Presumably those same naysayers want us to use green-screen monitors, have a crusty old mainframe in the basement and use telex machines for communications... but I digress.

Contrary to what people might tell you, Nirvanix' admittedly awful turn of events isn't a death knell for the cloud industry, any more than PRISM is (and more about that subject another time). What it is though, is a reminder that even with a move to the cloud and the attendant ability to focus on core business while third party minions tend to our infrastructure, there are still some requirements on customers to ensure that they, their data, and their organizations future remains secure.

Today some clarity came from Nirvanix, who tore down their website and left a statement telling customers how to get in touch with customer support. The statement helpfully advises customers that they need to actively participate in retrieving their data off Nirvanix servers and, interestingly enough, advises that Nirvanix has an [IBM](https://www.forbes.com/companies/ibm/) team ready to help customers. Many would say that this is too little, too late. That said, for Nirvanix customers, many of whom are in sheer panic about the terabytes of data they need to shift, any help is useful at this time.

I wrote a [post](http://diversity.net.nz/nirvanix-and-the-need-for-enterprise-due-diligence-oxygenclouds-third-way/2013/09/26/) last week setting out a couple of guidelines for organizations to avoid getting into trouble when outsourcing IT. While arguably the advice wouldn't have helped in this particular case, it's well worth revisiting and reiterative what it takes to be safe and secure when outsourcing IT to the cloud:

**Do Your Homework!**

The move to the cloud is an awesome thing – more flexibility, more focus, the chance to abstract non-core operations out to third parties – all the benefits we’ve been talking about for years. But with those very real benefits come some risks. Not risks that mean we shouldn’t use cloud at all, but risks that mean that the due diligence process is more robust than ever before. Things enterprises need to think about during DD include:

* Who is this vendor? Are they well funded and secure Will their business exist tomorrow and into the future? How much downstream damage would there be if they vanished into the ether?
* What are their SLAs? Is there an escrow agreement which covers the data in the event that they cease operations? Is there an agreed export model in the event that you want out? Is there an agreement in terms of notice periods?
* Do they have pre-existing arrangements with other parties that could help in the event that they go out of business

Now in the case of Nirvanix, it’s possible that DD wouldn't have uncovered issues – they were well funded, a “mature” player and had enterprise SLAs in place. But maybe their customers, given hindsight, would have been wise to negotiate hard for data escrow provisions or some other protections.

**Think Hybrid!**

I love the cloud – it has changed the world for the better and delivers massive opportunities for organizations. But with it comes some risks – we’re increasingly prepared to trust that our data, stored in third party locations, will always be accessible. But how realistic is this? Perhaps the onus is on us as customers to ensure that there is always a “Plan B”. Maybe we need to think about data storage in a hybrid way. Perhaps by using solutions that backup our data onto either another third party or to our own local storage (and yes, I know that will sound like heresy to some).

Fundamentally, customers need to stop and think about what happens to their data when they only have one storage provider and that storage provider has a major outage, or worse, goes out of business?

**Kay Takeaways**

The cloud is great. Outsourcing is great. Unreliable services aren't. The bottom line is that no one cares about your data more than you do - there is no replacement for a robust due diligence process and robust thought about avoiding reliance on any one vendor. Luckily there are many vendors in the marketplace who take the role of intermediaries - brokering service and storage across a number of different providers - judging by the press that one of these vendors, OxygenCloud, has been getting since the Nirvanix news hit, this is a model that more and more organizations are thinking seriously about.

Ben Kepes is a technology evangelist, an investor, a commentator and a business adviser. Ben covers the convergence of technology, mobile, ubiquity and agility, all enabled by the Cloud. His areas of interest extend to enterprise software, software integration, financial/accounting software, platforms and infrastructure as well as articulating technology simply for everyday users. Read more about Ben [*here*](http://www.diversity.net.nz/who-we-are-2/).