rackspace®

MANAGED VIRTUALIZATION

Powered By VMware®

How to Bring Shadow IT into the Light

8 Steps Along the Path

Contents

Executive Summary 2

Step 1: Take a Balanced View of Shadow IT 3

Step 2: Define What It Means to Bring Shadow IT into the Light 3

Step 3: Quantify the Shadow IT in Your Enterprise . . . 4

Step 4: Educate LOB Managers About the Business Risks. 5

Step 5: Meet with Each LOB Manager 6

Step 6: Consider Data Security Options 6

Step 7: Publish an Official Catalog of Apps 7

Step 8: Keep up the Momentum 8

Conclusions. 9

About Rackspace 9

Sources 9

How to Bring Shadow IT into the Light

8 Steps Along the Path

Executive Summary

The issue is control: IT has always controlled access to computing assets and data. But now the cloud has shifted control into the hands of the non-technical business user.

That user no longer has to wait for an overburdened IT department to meet their needs. With a phone call, or a few clicks of the mouse, that user can ask a cloud service provider to spin up a flexible solution, without the control—or even knowledge—of corporate IT.

That's why this dynamic has earned the nickname "Shadow IT." Nobody in the IT department even has to know it exists.

In short, the cloud has given business users a significant new measure of independence from the corporate IT department. But this freedom brings with it some significant business risks that IT leaders cannot ignore.

This white paper describes eight steps to help CIOs and other IT leaders bring Shadow IT into the light. And this paper points out that Shadow IT is not all bad—that in some ways it actually benefits the business. The key is to gain those benefits without risking the company's most valuable asset: your data.

Note that in this paper, the terms CIO, CTO, IT chief, and IT leader are used interchangeably.

Step 1: Take a Balanced View of Shadow IT

Shadow IT is on the minds of IT leaders, according to CIO Magazine's 2014 State of the CIO survey. Of the 722 IT leaders surveyed, four out of five said they feel IT projects done without IT involvement are creating problems.[1]

But is Shadow IT the real problem, or just a symptom? To answer that query, consider what gave birth to Shadow IT in the first place.

Since IT is considered a cost center, it is typically under-manned, under-equipped, and over-burdened with a backlog of time-devouring projects. According to Gartner, 80 to 85% of most enterprise IT budgets are consumed just by "keeping the lights on."[2]

With so few resources to focus on new projects, it's easy to see why business users view IT as slow and unresponsive to their demands. No one has time!

Even though this problem is not IT's fault, it is unacceptable. To remain competitive, every business needs innovative technology ready for end-user consumption, more or less on demand. And if users can't get it from IT, they will get it somewhere else. That somewhere else is third-party cloud services they can start up quickly with no engineer, no meetings, and no IT approvals.

So the real problem is not Shadow IT, per se. Cloud service providers deliver real value in a fraction of the time and cost it can take an internal IT department. And that's not always a bad thing.

IT leaders must take a balanced view of the benefits the cloud can offer. If they don't, business managers and users will continue to view IT as a barrier to innovation, and continue to look outside of IT for solutions.

Step 2: Define What It Means to Bring Shadow IT into the Light

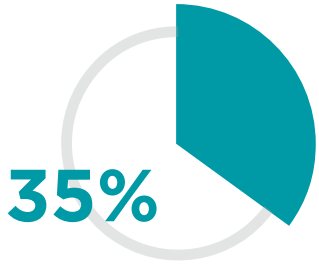
While some CTOs try in vain to root out all Shadow IT, astute IT chiefs take a more nuanced approach. They understand what the cloud has to offer: It's quick, easy, requires no IT resources, and provides compelling, pay-as-you-go OPEX pricing.

True, there are data security dangers that must be addressed. But once those are dealt with, the cloud can bring many benefits. In essence, the table is set for IT to guide the enterprise out of the conflict and toward a much-needed win-win.

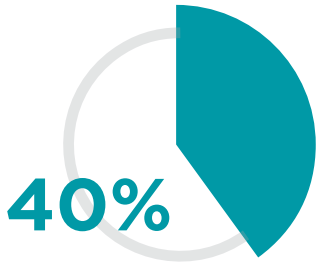
Consider what an ideal outcome would look like.

From the business user's standpoint, the preferred outcome is Shadow IT without the shadows. If a secret cloud instance doesn't quite work for them, they'd like to be able to ask their own IT team for support. But they're hesitant to do so when they've signed up for a cloud service in stealth mode.

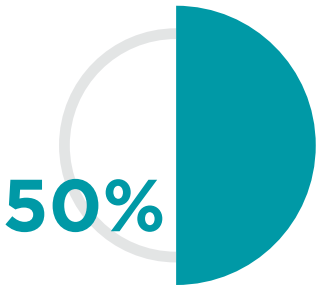
CIO ESTIMATES, 2013



GARTNER PREDICTS, 2015



CEB SERVEY, 2013



PWC SURVEY, 2011

Figure 1: The Size of Shadow IT—Four Estimates

Note: Teal areas show Shadow IT as a percentage of Formal IT budget

From IT's perspective, the preferred outcome is minimal security risk. The thought of sensitive data leaving the safe confines of the company firewall naturally makes every CIO nervous.

The best-case scenario is a combination of these two ideals: flexible, on-demand cloud services that adhere to IT's high standards of security and data governance.

By reconciling agility with stability, the CIO can transform the logjam of Shadow IT vs Formal IT into a more productive paradigm. Under this new model, IT can serve as a service broker to find, scrutinize, and approve the best cloud services that give business users what they need.

Step 3: Quantify the Shadow IT in Your Enterprise

No one can say for sure how big Shadow IT really is, as shown in Figure 1. But it's a lot bigger than most CIOs estimate, when they count it as 20% of their budgets. Other surveys and estimates peg Shadow IT at up to 50%--or more—of formal IT budgets.

A 2013 study by Stratecast/Frost & Sullivan survey reveals that for every 20 SaaS apps used, seven are unapproved by IT.[3] That's 35%–precisely what Gartner predicted in 2011.[4]

Getting knowledge workers to admit to using Shadow IT in an anonymous survey is one thing. Getting them to admit it to their own IT department is quite another. They know they shouldn't, and expect that being caught will involve consequences.

But that's a risk they're willing to live with. The pressure to get their jobs done outweighs any concerns about complying with company IT policies.

To bring Shadow IT out of the shadows, IT leaders must know what unauthorized services are being consumed and what corporate data is being sent into potentially unsecured cloud repositories. But how can you see in the dark?

Here are three tactics to help see how big your Shadow IT problem really is:

- Review bills with the cooperation of your accounting department. Unless a user paid for cloud service with their own credit card, Accounts Payable and expense reports will show any ongoing services being charged to the company.
- Use a network scanning and detection tool; several have been written expressly to help IT teams uncover shadow IT.

Data Breach Business Risk Cost:

$188

average cost per compromised record of a data breach to a U.S. company

$3M

US companies' cost of lost business due to data breach

- Examine your actual outbound traffic reports looking for large, frequent, or unexplained interactions with off-premises services.

Don't be surprised if you discover a significant slice of IT spending happening in the shadows.

Step 4: Educate LOB Managers about the Business Risks

When employees use a desktop utility with no outbound web communication, there's not much cause for concern. However, today's SaaS offer a captivating array of helpful apps available any time, anywhere—on the road, from the home office, even from a crowded café at an airport.

The problem, of course, is that almost all these utilities ask the user to send mission-critical company data into a cloud-facing data store with the potential to get a company and its CIO into big, big trouble.

For example, the "2013 Cost of Data Breach Study" from The Ponemon Institute shows the average cost of a data breach to a U.S. company was $188 per compromised database record.[5] When you consider that today's databases house millions of records, it's easy to see how even one breach can trigger an astronomical loss.

In fact, this study shows the average cost of lost business to U.S. companies was a shade over $3 million per incident. These costs include customer turnover, more efforts required to acquire customers, damage to brands and reputations, and diminished goodwill.[6] No CIO wants all that on their conscience.

Corporate users seldom consider these pitfalls when they use cloud services, and they're certainly not trained to evaluate any service provider's security. If a SaaS company tells them that their data will be secure, that's enough to satisfy any user.

Therefore, CIOs must educate their line-of-business (LOB) managers on the risks they could be exposing the company to when they approve cloud-based Shadow IT.

Some CIOs write and publish IT security warnings to company intranets. Others have been known to compile threat statistics into chart form and disseminate them at management meetings. These methods, however, often fail to bridge the communication gap; many corporate managers are not technical enough to understand what IT threat metrics mean or what action they should take.

Therefore, the most effective means of educating LOB managers is an informal one-on-one meeting to explain the risk Shadow IT truly represents.

Step 5: Approach Each LOB Manager

Armed with talking points on the risks of Shadow IT, the time has come to meet with each of your LOB managers.

The agenda can be straightforward:

- We know some of your people are using cloud services without IT's approval
- Here's the risk to the company
- A big part of IT's job is to safeguard the data we're entrusted with
- We'd like to find a way to give your people what they need, while we do our job of protecting our data

This conversation doesn't need to be as uncomfortable as you might think. The outcome of each meeting will hinge on the tone you set. That tone should be all about adding business value through technology, not scolding people for doing something sneaky.

Todd Coombes, CIO of Indianapolis-based CNO Financial Group understands this well.

"If I were to take a hard line and say, 'no Shadow IT,' I'm not going to be adding any value for my business partners, and it will create resentments and wreck relationships," he told *ComputerWorld*.[7]

The goal for each meeting is to understand how IT can enable a certain group of business users to use the cloud safely. Nobody is in a better position to make this call than the Chief Technical Officer.

The outcome of each meeting can be very positive on two fronts. First, each LOB manager can realize that IT can help them use the cloud, not hinder them. Second, IT can understand the motivation for using cloud services, and have good reason to assemble a pool of alternatives that are cost-effective and safe.

Step 6: Consider Data Security Options

Next, it's time to address the single biggest risk of Shadow IT: security and governance. To do this, IT must specify a cloud governance framework used to evaluate all prospective cloud providers.

Only vendors who meet these published security standards can earn a spot on the list of company-approved cloud service providers (CSPs).

As you consider your options, look for the architectural elements that are proven effective in safeguarding sensitive data in the cloud.

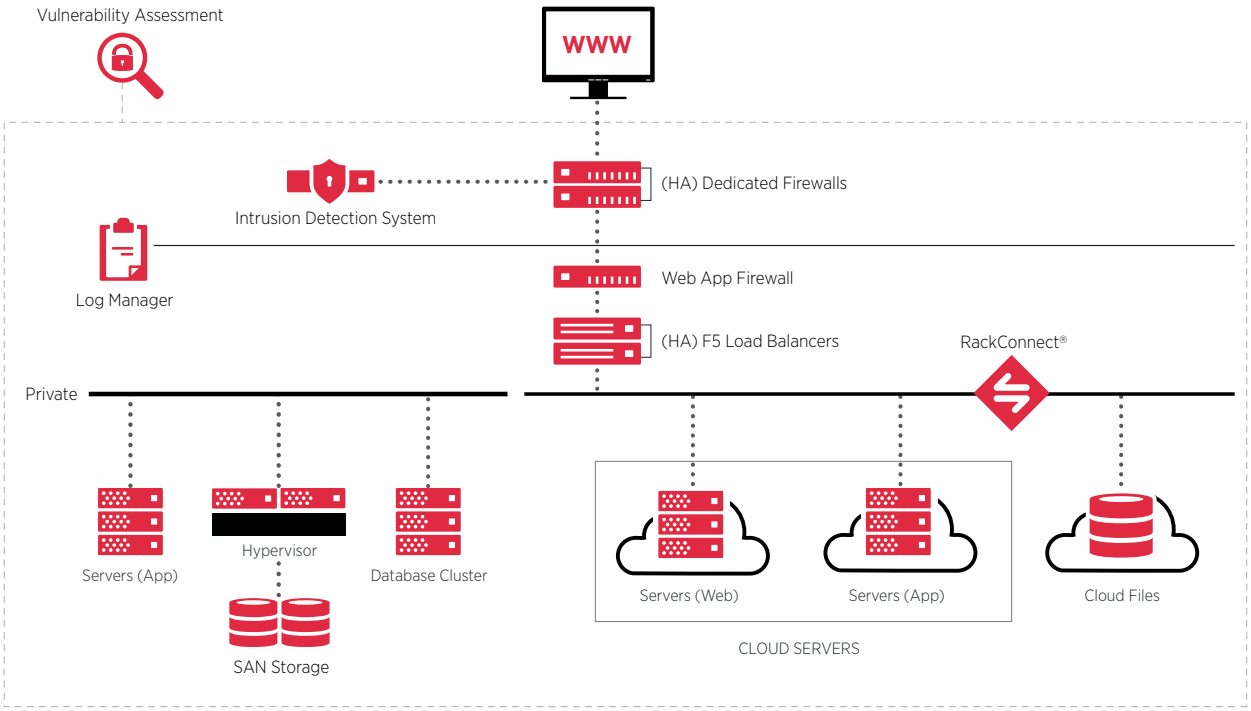


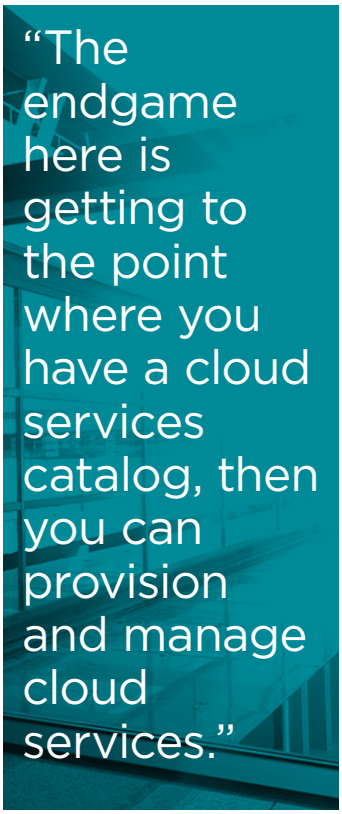
Figure 2: Data Safeguards in the Cloud

As shown in Figure 2, a secure architecture for cloud applications generally uses these six common components:

1. **Dedicated Firewall** – the first line of defense against external attack
2. **Intrusion Detection System** – gives IT real-time visibility into potential threats
3. **Vulnerability Assessment** – identifies exploitable weaknesses in the system
4. **Web Application Firewall** – blocks non-essential traffic from reaching the application layer, and protects applications from malicious code
5. **Load Balancers** – by normalizing TCP traffic, these lessen the vulnerability of any individual server and make it easier to detect evasion network attacks
6. **Log Management** – beyond audit and accountability, logs can help IT respond to attacks and shorten recovery times

For more discussion of these components, see the Rackspace white paper called "Reference Architecture: Enterprise Security in the Cloud."

Providers who build cloud services with these components stand a much greater chance of providing a secure yet functional user experience.



Step 7: Publish a Catalog of Supported Apps

The next step is for IT to research and compile a list of approved cloud service options for business users to choose from.

“The endgame here is getting to the point where you have a cloud services catalog,” said a recent article in CIO, noting then “you can provision and manage cloud services in the same way you provision and manage your own data centers and colo facilities.”[8]

IT should categorize this catalog by department and cloud functions. The published list should be accompanied by clear, step-by-step instructions on how to provision a new instance. And it should list the managers with authority to purchase cloud services and assign permissions to users.

With this catalog, the CIO will begin to transform his department into a true cloud service broker. IT will no longer be known for creating obstacles, but for supporting smart services. With a self-service model in place, corporate IT will have more time to spend on strategic initiatives that deliver true business value, instead of just keeping the lights on.

It’s ironic that this major step forward was born out of Shadow IT. That’s the way it worked for Brian Lillie, CIO of Equinix Corporation.

“Instead of us throwing up roadblocks, we said, ‘Let’s enable this and give these guys a way to exploit it,’” he says. Non-IT people assembled what he calls “a very slick sales tool” that measure network latency across company operations in 13 countries. He notes that getting out of the user’s way requires a mind shift for IT. “But people are creative and … breakthroughs can come from anywhere.”[9]

Once you’ve established your catalog of supported vendors and cloud services, make popular apps available through your enterprise portal.

Or even better, set up an enterprise app store: a centralized directory for services, applications, and APIs available with a click or two. That’s no longer a novel idea: 44% of IT leaders surveyed either have, or would like to have, a company app store. [10]

Step 8: Keep Up the Momentum

Now that you’ve come to terms with your company’s shadow IT, why not keep up the momentum?

Continue to meet with your LOB managers regularly to assess their satisfaction with the selection of cloud services available in your catalog or through your portal. Over time, you may want to anticipate and pre-offer further cloud services, based on the most-requested features you hear about from your LOB managers and users.

You'll probably want to repeat steps 3, 4 and 5 from time to time—perhaps every quarter—to continue coaxing more shadow IT into the light… or at least keep up with the ongoing draft back into the shadows.

And since you're not trying to stamp out shadow IT entirely—remember?—this ongoing process can be a healthy exercise in discovering what your users want and where they're getting it. Then you can try to keep ahead of most of them with your approved cloud offerings.

Conclusions

This white paper shows how IT can give users the ideal solution: a pool of cloud services they can access with a phone call or through a central portal, while maintaining acceptable standards of security and compliance.

With a catalog of approved vendors in place, the CIO can relax a little, knowing that whatever enterprise data is in the cloud is secure. Business units can be more self-supporting, and users will have no reason to look elsewhere for solutions.

Bringing Shadow IT into the light can be challenging. But you don't have to do it alone. Your Rackspace consultants have years of experience helping CIOs get control of Shadow IT, while giving managers and end users the services they want. ***Call Rackspace at 800-961-2888 to get started today.***

About Rackspace

Rackspace® (NYSE: RAX) is the global leader in hybrid cloud and founder of OpenStack®, the open-source operating system for the cloud.

Hundreds of thousands of customers look to Rackspace to deliver the best-fit infrastructure for their IT needs, leveraging a product portfolio that allows workloads to run where they perform best—whether on the public cloud, private cloud, dedicated servers, or a combination of platforms. The company's award-winning Fanatical Support® helps customers successfully architect, deploy and run their most critical applications.

Headquartered in San Antonio, TX, Rackspace operates data centers on four continents. Rackspace is featured on Fortune's list of 100 Best Companies to Work For.

For more information, visit www.rackspace.com

Sources

1: "2014 State of the CIO Survey", CIO, January 2014, page 1, retrieved 21 May 2014 from http://www.cio.com/documents/pdfs/StateoftheCIO2014.pdf

2: Christy Pettey, “Gartner Says Eight of Ten Dollars Enterprises Spend on IT is ‘Dead Money’”, Gartner Group, 9 October 2006, retrieved 21 May 2014 from http://www.gartner.com/newsroom/id/497088

3: Stratecast/Frost & Sullivan,“The Hidden Truth Behind Shadow IT”, Macafee, November 2013, retrieved 21 May 2014 from http://www.mcafee.com/us/resources/reports/rp-six-trends-security.pdf

4: “Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond”, Gartner, 1 December 2011, retrieved 21 May 2014 from http://www.gartner.com/newsroom/id/1862714

5: “ 2013 Cost of Data Breach Study: Global Analysis”, The Ponemon Institute, February 2013, page 5, retrieved 21 May 2014 from http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis

6: Ibid, The Ponemon Institute, page 17

7: Julia King, “The Upside of Shadow IT”, ComputerWorld, April 2012, http://www.computerworld.com/s/article/9226415/The_Upside_of_Shadow_IT

8: Thor Olavsrud, “How to Bring Shadow IT Under Control”, CIO, January 2014, retrieved 21 May 2014 from http://www.cio.com/article/746441/How_to_Bring_Shadow_IT_Under_Control

9: Ibid, Julia King

10: Joe McKendrick, “10 good arguments for enterprise app stores”, ZDnet blog, 20 April 2014, retrieved 21 May 2014 from http://www.zdnet.com/10-good-arguments-for-enterprise-app-stores-7000028588/

Sources for Figure 1 Piecharts

Chart 1: CIO estimates from “CIOs blind to 40 percent ‘shadow’ IT spending at their firms”, ComputerWorld UK, 28 November 2013

Chart 2: “Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond”, Gartner, 1 December 2011

Chart 3: Tom Groenfeldt, “40 percent of IT spending is outside CIO Control”, Forbes.com, 2 December 2013

Chart 4: PriceWaterhouseCoopers’ Digital IQ Survey, quoted by Julia King in “The Upside of Shadow IT”, ComputerWorld, 23 April 2012

Toll Free: 1.800.961.2888 | International: 1.210.312.4700 | Or Visit Us www.rackspace.com

Rackspace® | 1 Fanatical Place | City of Windcrest, San Antonio, Texas 78218 U.S.A | DATE MODIFIED: 08072014