The Cloud checklist for SMBs: 7 tips for safer Cloud computing

Make sure your company's data is as secure as the rest of your endpoints with these 7 helpful tips on how to stay safe in the Cloud.

By Cameron Camp, Security Researcher

The Cloud concept, a flexible Virtual Machine (VM) based system that allows rapid expansion and dedicated functionality without hiring new staff, has taken the business world by storm. The reasons are many, from the small business perspective, including things like the ability to outsource specific business processes that may not reside at the core of your expertise, or the ability to just "hit a button" and have a ready-to-go server at your disposal, without the accompanying in-house expert and hassle.

While this new packaging of a technology that's now almost 10 years old (in its current iteration, others are much older) has made some things much easier for small business, could it undermine the security of you and your business (and your data)? The answer depends on several variables, including your business need.

In this tech brief, we'll cover a few of the things you should check into before trusting your data to the Cloud. We've compiled 7 tips, items that should be on your checklist before you make the leap, and a few things to watch out for along the way.

1. Know your Cloud provider

In the deluge of recent-comers to the Cloud market, it's important to check the credentials of your chosen provider to know what you're getting, and not getting. For instance, does the firm have a long history of solid security, or is it still a bit of a wildcard? If a firm has a commitment to security and a history of executing security on their more traditional servers, it stands to reason that they'll merge that commitment with their Cloud-based offerings as well. The old adage that you get what you pay for applies here, and for good reason. It takes work to get security right, and work translates into experts and quality hardware, neither of which are free.

2. Define your business need

Getting by on a friendly recommendation combined with believing the buzz isn't enough. Make sure you can clearly articulate a good business fit for a Cloud setup. If you want very fast low-latency communication between your office and the Cloud, you may be in for an unpleasant surprise. While storing files might work well for the Cloud, database queries

> Encrypt your bits and bytes. Both at rest and in transit, encrypt as much of your Cloud data and traffic as you can get away with.

Limit access to specific individuals and don't just leave the connection open for everyone to use. Consider two-factor authentication instead of merely relying on passwords.

from your in-house staff to the Cloud can seem like adding light years to your business process response times. If you have a critical business intelligence real-time app, it might be worth a second opinion to see whether the Cloud is right for you. At least be prepared to bring some optimization expertise to the table when shifting processing to the Cloud. (And consider whether or not you would be better served by a local server dishing up virtual machines.)

3. Encrypt your bits and bytes

Both at rest and in transit, encrypt as much of your Cloud data and traffic as you can get away with. It adds a layer of complexity and a little processing overhead, but not much (after you get it established), and the peace-of-mind will be worth it in the end. Not sure how to do this? Talk to your provider about the best ways, and ask around, you're likely to find someone with experience to help you, even if you're a small business on a tight budget. And, of course, test the setup before you go putting the "crown jewels" out there in the ether.

4. Manage your Cloud access

Because putting your data and/or processing in the Cloud means it is one step removed from your physical control, and because Cloud content can often add up to a lot of valuable intellectual property and sensitive information, you need to make sure you control who can access it. Your Cloud provider may promise to look after your data, but that does not relieve you of responsibility for policing the access you authorize. It's a good idea to limit access to specific individuals that need access, not just leave the connection open for everyone to use. Consider two-factor authentication instead of merely relying on passwords.

5. Backup your Cloud data

Depending on your use case, you may be backing up data to the Cloud, or using it for any number of other processes. But here's the kicker: Have you checked and tried to restore your data from the backups, or is it "out of sight, out of mind?" If you haven't, sadly, you're in the majority. I know it seems simple, but occasionally try to get access to a critical file and restore it (locally or across the network) to your machine. Did it work? Many find out after their local hard drive grinds to a screeching halt that their backups also did some time ago. This is usually followed by a series of frantic steps. If you take a few minutes and see that your data is duplicated, whether data you access daily that's stored in the Cloud, or Cloud-based backups, and you can still retrieve it, you'll be miles ahead in confidence and know that if something bad really did happen, you'd be protected.

6. Check the fine print for your Cloud

As my colleague, Stephen Cobb, pointed out a few months ago, the terms and conditions of your Cloud agreement should be read very carefully. Consider two sections of the Amazon Cloud Drive Terms of Use, which are not that unusual in the Cloud business:

> **5.2 Our Right to Access Your Files.** You give us the right to access, retain, use and disclose your account information and Your Files: to provide you with technical support and address technical issues; to investigate compliance with the terms of this Agreement, enforce the terms of this Agreement and protect the Service and its users from fraud or security threats; or as we determine is necessary to provide the Service or comply with applicable law.

ESET BUSINESS SOLUTIONS

ESET Endpoint Solutions

ESET Endpoint Antivirus (Windows/Mac*/ Linux*)
Antivirus / Antispyware

ESET Endpoint Security (Windows)
Antivirus / Antispyware / Firewall / Antispam

ESET Mobile Security (Windows Mobile/Symbian)
Antivirus / Antispyware / Firewall / Antispam

ESET Server Solutions

ESET Mail Security (Windows/Linux)
Antivirus / Antispyware / Antispam

ESET File Security (Windows/Linux)
Antivirus / Antispyware

ESET Gateway Security (Linux)
Antivirus / Antispyware

*ESET NOD32 Antivirus Business Edition Mac OS X,
ESET NOD32 Antivirus 4 Business Edition for Linux

Check the fine print: Cloud providers typically provide minimal liability for your files and require that you maintain appropriate security measures.

5.3 Security. We do not guarantee that Your Files will not be subject to misappropriation, loss or damage and we will not be liable if they are. You're responsible for maintaining appropriate security, protection and backup of Your Files.

Will that work for you? Will that violate promises about privacy that you have made to the folks whose data you plan to place in the Cloud? Can you get your Cloud vendor to change their standard terms-and-conditions to get your business? These are important questions you need to ponder on your path to the Cloud.

7. Remember, viruses can live in Clouds

Recent news that the malware known as Crisis has been infecting VMware virtual machines reminds us that the Cloud does not possess special immunity from malware (ESET antivirus products identify Crisis as OSX/Morcut.A and have been defending against it since last month). We should point out that Crisis affects Type Two hypervisor deployments, not the Type One more typically used in large cloud deployments, but the fact remains that moving to the Cloud does not end the need for antivirus protection; and you still need strong endpoint security on those devices that are permitted access to your Cloud (going without would be a risky strategy that could prove costly).

Cloudy Conclusions?

Of course, in the end it's a case-by-case decision as to how much and what type of information your business or organization will put in the Cloud. But if you keep in mind these 7 points for securing your slice of the Cloud, we think you'll have a much more pleasant, and secure experience. For further thoughts on the subject here's a recent podcast recorded about cloud computing (.mp3) from ESET.

*Stay up to date with the latest Internet threats—visit **blog.eset.com***

*Protect your digital privacy with ESET. For more information on your security options, go to **eset.com***

ESET North America
610 West Ash Street
Suite 1700
San Diego, CA 92101

Toll Free: +1 (866) 343-3738
Tel. +1 (619) 876-5400

www.eset.com