Realtime publishers

Using Cloud Services to Improve Web Security

The Essentials Series

Can You Trust a Cloud-based Security Solution?

sponsored by webroot®

Mike Danseglio

Copyright Statement

Can You Trust a Cloud-Based Security Solution?

Cloud computing and security services seem like they would never go together. The former is a function that exists somewhere outside the host, outside the network, and is tapped when needed to perform a certain function such as data archival. The latter is a mindset, an approach that pervades throughout every facet of an IT infrastructure. So can they go together?

Yes they can.

As the previous article explored, cloud computing offers great benefits when used to provide security services. Beyond the numerous core benefits of cloud computing, security solutions delivered in this way are frequently more portable, more stringently managed, and more difficult to compromise than dedicated on-premise solutions. They also offer the option to assign risk to a trusted third-party provider.

Risk Assignment

On first glance, many IT professionals read the term *risk assignment* as something bad. Almost as if they're using it as an excuse to not secure a resource. But risk assignment is a core trait of any security plan. There are simply some threats that are not worth securing with traditional security measures but must still be addressed in some way.

A common example of risk assignment in daily life is car insurance. Most of us pay for insurance that covers our car, the occupants and contents of our car, and any other car we collide with. If a collision occurs, the insurance companies resolve the situation by repairing or replacing the cars and paying for medical attention to the occupants. It isn't just required by law; it is a good idea. We assign the financial risk of a collision or injury to a third party and pay them a fee to accept the risk. The alternative is to always keep enough cash on hand to pay full value to replace vehicles and cover medical expenses whenever a collision occurs—or risk a lawsuit.

The IT security version of this situation isn't far off. The difference is that, in the cloud security service case, the risk assignment is accompanied with measures to prevent attacks. It's analogous to your insurance agent charging a bit more for a better policy and assigning a police car to lead you wherever you drive. You could still have an accident, but it is far less likely. And probably worth the extra money.

The key differences between cloud security solutions really lie in two categories: the company providing the service and the features of the service. Both need to be examined to make a reliable decision on whether to trust cloud computing for a security solution.

Cloud Security Service Providers

When cloud computing began its rapid expansion, it brought a number of companies to the forefront of IT's attention. It seemed that overnight virtually any company that provided a data center–type solution had become a cloud computing service provider, and that any service-oriented solution was now a cloud computing solution.

Such was not quite the case for cloud-based security services. Security companies took a bit more time as they really examined whether they could make good on an offer to provide security services in this new way. Cautious changes are the hallmark of good security providers, and relatively few jumped quickly. With security, there's often no "ramp up" time—if the solution isn't secure, attackers will not patiently wait for a patch or give a company a second chance.

Caution shown by cloud security service providers benefited the market. The result is that cloud-based security solutions in today's market tend to be more dependable than other cloud solutions, even early in the service's first few versions.

When selecting between cloud security solutions, you should take a long, hard look at each company providing the solutions. Many of the big name companies will garner instant name recognition and require little research. Others will take a bit of investigation but may be well worth the time spent. There are a few areas to which you should pay particular attention when looking at cloud security service providers.

Reputation

Every provider you consider should be established in the market. That means that other people are already using their services and have some feedback. With the Internet, it is a simple matter to find feedback from your peers, solicited or not, on virtually any service and company.

Considerations for a company's reputation in the cloud security space should include answers to these core questions:

- Does the company respond to clients quickly and effectively?
- Does the company have a strong track record in both the security and service fields?
- Are others happy with the company's products and support services?
- Has the company successfully defended against emerging threats recently?

You probably noticed that these are all qualitative questions. Reputation is a very subjective aspect. In the end, when you have answers to these questions, you should have a "gut feel" for the reputation of a company.

Service Level Agreements

You can use several terms to describe these arrangements; Service Level Agreement (SLA) will suffice as a broad description. What an SLA boils down to is the responsiveness of the provider. An SLA defines how quickly and thoroughly the provider will respond to a threat. If you've worked with such agreements before, you know that these can vary widely across industries, services, and financial agreements.

Typically, you want to seek out cloud-based security providers that offer an SLA that meets your existing security requirements. Lowering your security expectations to correspond to an SLA should never be considered. Having said that, you shouldn't enter into SLA discussions with unreasonable expectations (for example, a 15-second in-person response time and assessment for all levels of attack, 24 hours a day)—or you should expect to pay a hefty mark-up to have those expectations met.

When discussing an SLA with a provider, have handy a list of regulations that apply to your company and industry. Most likely, the provider also has an idea of the regulations that impact you and knowledge of how those map into a specific response framework.

Financial Reliability

As mentioned earlier, you are in essence assigning some quantity of risk to a cloud security provider by using their service. But what good is assigning risk to an insolvent organization? It may be gone in a short time or may not carry enough financial backing to support the company when the situation isn't perfect.

This is akin to taking out car insurance from a company with no financial or legal backing. The first significant accident or lawsuit will cause the business to fail, and the owners will disappear or hide behind bankruptcy laws.

Only select a solvent security service provider that has a strong financial history. This is very similar to selecting other service providers on the same basis, so I won't go into an exhaustive description. You likely know how to research a company's financial position all too well, and there are numerous tools to help you.

Cloud Security Service Features

Along with analyzing the service provider, you will need to determine whether the technical features of the service meet your expectations. For most people, a cloud-based Web security solution is a new addition to the IT environment. Thus, it helps to understand which features are common and should be expected.

Integration with Existing Security

Virtually every IT environment has some quantity of technical security measures in place. The most commonplace components include network firewalls, email spam filters, and host-based malware scanners. More advanced networks integrate components such as intrusion detection systems, stateful inspection firewalls, and proxy servers.

When you consider adding a cloud-based security service, first determine whether the service will interfere with any of your existing security infrastructure. This situation could make things difficult during deployment or result in a loss of investment. For example, if you're testing a cloud-based Web security provider and every SSL-protected Web site access causes your proxy server to generate a security warning, you must determine how to address the warnings. Simply ignoring the matter will cause a security issue in the future when legitimate threats are mistakenly ignored and users are redirected to spoofed SSL sites.

Simplicity

Succinctly stated, complexity is the enemy of security. Usually, the simpler the solution, the more effective it becomes. This axiom holds true across virtually every aspect of security.

Most cloud-based security solutions are simple in nature. They add on to an infrastructure or client configuration and are imperceptible to the user. Invisible security controls are the most effective in protecting users because users see no need to circumvent them, complain about them, or manage them in any way.

Compare this reality to traditional host-based and network-based security controls. These controls often require manual intervention to resolve issues, update signatures, authorize infection removal, and so on. These tasks cost the company time and money in user, Help desk, and IT effort.

Flexibility

Every organization has different security needs. Some simply need malware or spam prevention. Others may want content filtering to prevent users from accessing adult content via work assets. Still others may have regulatory needs to block access to competitor's data or limit the information flowing out through Web sites. Most cloud-based Web security solutions recognize and embrace these needs. You should ensure that whatever Web-based solutions you consider are flexible enough to enforce *your* business rules and policies. If the only option is to accept a pre-made content framework, seek another option.

Summary

Many IT professionals have concerns about trusting their company's security and compliance needs to a solution in the cloud. These concerns were valid in the past, but today's cloud computing environment makes this option, and its many benefits, a viable choice. Even a quick glance at the strong benefits provided by a cloud-based Web security solution will have you considering this approach for your company's security and compliance needs.