Market Report

Protecting a Cloudier Future

Cloud Protection a Key Enabler for Inevitable Clouds

By Evan Quinn, Senior Principal Analyst

November 2012

Fast Forward Five Years: Cloud Becomes the Standard

The use of cloud as a deployment alternative for IT infrastructures, application platforms, and applications has evolved over the past decade from novelty, to proof-of-concept, to pilot, to a fundamental instrument in IT's toolbox. Despite cloud's ascension thus far, we will likely look back five years from now and realize that we currently only stand at the threshold of cloud's acceptance. As we approach 2020, will Cloud and on-premises have swapped roles? Will cloud, due to its speed of deployment, scalability, elasticity, and preferred financial model eventually become IT's primary deployment model? The answer is likely "yes," pending two developments in the evolution of cloud.

Widening the Path to Cloud Requires PaaS and Protection

What stands in the way of cloud continuing its advance? It has been oft-stated that security ranks as the number one hurdle IT departments cite as preventing a more rapid adoption of cloud. While ESG agrees with that assertion, we also believe that application platform and development technologies, associated with Platform-as-a-Service (PaaS), the middle tier of cloud, have trailed the progress of the infrastructure and application layers.

Without PaaS adoption, cloud services only go so far. For example, it is difficult to imagine a fully functioning big data analytics facility in a cloud without PaaS. PaaS enables customization, organization-specific versus vanilla processes, and a way to span technology silos. ESG believes, however, that PaaS is gaining momentum, and the result will mean that in a few years IT will have access to a wider variety of more fine-grained cloud services to choose from—some of their own making, some from third-party sources.

The advance of PaaS, and on-going advances and acceptance of cloud at the other layers, suggests that five years from now every IT department will lean more significantly on cloud computing: IT will deal with more clouds, more cloud services, and perhaps the notion of "cloud" as something unique will disappear entirely because it will become the default computing fabric.

But how does the advance of PaaS and general adoption of cloud impact security, or perhaps a more concise term than "security" is "protection," which remains the primary hurdle for cloud usage? ESG prefers the term "protection" in the cloud context, because it suggests a higher order level of responsibility and function—it includes security and closely related technologies such as information management. What types of protection will be required to enable the advance of cloud? If cloud computing adoption, at all three layers, marches forward at a rapid rate of speed with PaaS enabling a richer set of clouds and services, protection technologies will need to do more than just keep up—cloud protection technologies need to up-shift from being a hurdle to being an enabler.

Elements of Cloud Protection: Policy, Identity, Information, and Infrastructure

What are some of cloud's characteristics that make it a unique challenge from a protection perspective? One challenge involves ownership—not just who "owns" a cloud, but who owns the access to, data in, and processes through the cloud. Another challenge has to do with inter-cloud data flow, or cloud to non-cloud resource sharing. And the multi-tenant nature of applications and application platforms raise protection questions germane to cloud computing. Let's distill these challenges into specific feature sets that protection technologies must address in order to give us safe clouds.

- ***Policy***: The ability to capture, house, manage, distribute, and apply policy stands out as a key requirement for cloud computing. Compliance requirements dictate the need for policy definition, and a best practice for an organization's adoption of cloud is to develop and manage a set of cloud-specific policies. Storing ownership and access rules, preferably in the cloud for clouds, is utterly fundamental for cloud protection. How an organization chooses to address the sensitive topic of information privacy in the cloud is expressed and captured as policies.

- ***Identity***: Given established cloud policies, identity management acts as the first and fundamental step to apply the policies. Identity protection features that manage the definition of who you are, your role(s), the policies under which your access to clouds operate, and how you must authenticate, bridge the entire range of cloud protection from policy management to information protection. Notice that in this era of a massive number of new endpoints, applying identity management through the cloud provides a single, convenient means to manage identities regardless of device or location of cloud consumption.
- ***Information***: Once policy has been defined for, and ownership and access have been granted to information, technologies are required to keep the relevant information protected per policy, specifically in terms of data sharing and data availability. Examples include encryption and data loss prevention that offer protection in the sharing domain, and back-up, restore, and e-discovery which ensure information availability and compliance.
- ***Infrastructure***: While the first three areas of cloud protection involve mainly detailed protection around groups of users, individual users, and discrete information and services, what happens with more generalized protection requirements? What, for example, protects against a cloud breach or outage? How does one monitor a cloud infrastructure to detect and prevent an advanced threat attack? What availability and scalability technologies do you deploy in a cloud infrastructure to ensure that peaks are handled, and local outages do not turn into general outages?

The Bigger Truth

It doesn't matter where organizations deploy information technology—from smartphones to supercomputers, from LANs to the entire Internet, from server farms to global clouds: Policy management, identity and information management, and the ability to secure infrastructures form the axis of protection. Clouds, however, present a new paradigm for implementing these four areas of protection. But like cloud computing itself, there are considerable benefits to doing the cloud protection job right.

By effectively implementing protection for clouds, you mitigate the needs for protection in other areas of computing. For example, by using protection in the cloud for your clouds, the improperly forwarded sensitive information may never reach the endpoint of consumption. Similarly, advanced attacks stopped at the cloud infrastructure layer mitigate the need to deal with compromised endpoints. And ultimately it doesn't matter which clouds, information, infrastructure, and endpoint are involved—a consolidated, virtualized cloud-based protection resource ensures that your organization's policies can be applied across your IT assets, regardless of location.

In that sense, that notion of elasticity which makes cloud computing so appealing applies to cloud protection as well: Administration can take place regardless of physical location, and a policy change can instantly be applied across all of your clouds, or across those clouds to which it applies. Most CISOs and CIOs understand that excellent cloud protection products, implemented effectively, reduce the pain of protection across their asset base. What they may also realize is that effective cloud protection solutions open up the benefits of cloud computing to their organizations more rapidly, and thus cloud protection technology becomes a key enabler for the on-going adoption of cloud computing.

Enterprise Strategy Group | **Getting to the bigger truth.**

20 Asylum Street | Milford, MA 01757 | Tel: 508.482.0188 Fax: 508.482.0218 | www.esg-global.com