



Richard Stiennon, Contributor

Evaluating vendor cloud security strategies

from <http://www.forbes.com/sites/richardstiennon/2011/10/31/evaluating-vendor-cloud-security-strategies/>

It is well documented that there is a difference between strategy and tactics yet the two are often confused. As IT infrastructure is overwhelmed with the “move to the cloud” every vendor of security products is tasked with coming up with a cloud strategy. In my mind tactics are based on “what do we have and how can it be virtualized?” whereas strategy is based on “what do customers need and how can we deliver it?” I have observed four approaches to cloud security strategy:

Sell more gear to support cloud initiatives. This is the approach being taken by the big network equipment vendors. They have fallen behind on the security front as their products are getting long in the tooth and they missed the rise in threats while ceding ground to upstarts. Let’s call them C&J Big Iron, Inc. Just as their strategy throughout the Internet boom years was to sell more big routers and switches to ISPs and carriers their current strategy is to be part of big cloud projects and continue to sell big iron to big projects. But do not be fooled by their cloud security strategy. They may have components of SaaS and virtualized software but they have not figured out the big picture yet.

The second level of cloud strategy for security vendors is to virtualize their software platforms so that enterprises deploying virtualized environments can use the many CPUs and servers they have deployed without introducing the specialized hardware appliances that were the hall mark of network security for the last decade. Those vendors whose products ran on plain vanilla servers have been the first to make the switch. Many of them are also moving to a hybrid product offering whereby they provide a hosted management platform, usually within their own private cloud.

The third strategy is Security as a Service. This is a true cloud implementation and is best suited to consumer and SMB solutions although there are cloud based DDoS defense services that target the larger enterprise. The dozens of vulnerability scanning services that have sprung up in the wake of PCI DSS requirements for quarterly scans are the best example. Hosted web content filtering, VPN, and authentication are also coming in to their own.

There is only one vendor I have identified which has jumped wholeheartedly into the cloud with a well defined cloud strategy. Trend Micro started talking about their goal of securing cloud environments over three years ago and not only has stayed constantly on message but has executed on their strategy. The most important move was the acquisition of Identum, one of the first movers in identity based encryption. Encryption of course is key to hosting data and processes in the cloud. But traditional PKI with its chains of trust and key management issues is already cumbersome to implement in traditional environments. Extending PKI to the cloud only exacerbates the issues. Identity based encryption (IBE) is a simple concept that uses an identity record (an Active Directory entry or simply an email address) to generate and retrieve encryption keys. It is the basis of Trend’s Secure Cloud offering. With it an enterprise can safely host their data and virtual servers in any cloud environment while retaining control of the keys. Regardless of the assurances of a cloud provider about their security if your data is not encrypted it is not safe. With Secure Cloud you could architect a cloud service even on Amazon EC2 and rest easy that your data was secure.



Trend has also built on their traditional strength in server protection by acquiring Third Brigade and its Deep Security protection product, which can either reside on one VM on a host machine to protect all the other VMs or it can be bundled with each VM to provide firewall, anti-malware and host IPS.

The final requirement for Trend's cloud strategy is tight integration with the virtualization technologies and they have accomplished this with a partnership with VMWare and integration with Citrix XenServer, and Microsoft HyperV.

The cloud is disruptive to the IT space which is a good thing as increased flexibility, efficiency and yes-security, is possible. All security vendors are developing cloud security product strategies. They will have to move fast to catch up with Trend Micro.

To hear Trend's founder describe their strategy watch my interview with Eva Chen filmed earlier this month.



Full disclosure. I write position papers for many vendors of security products including Trend Micro.