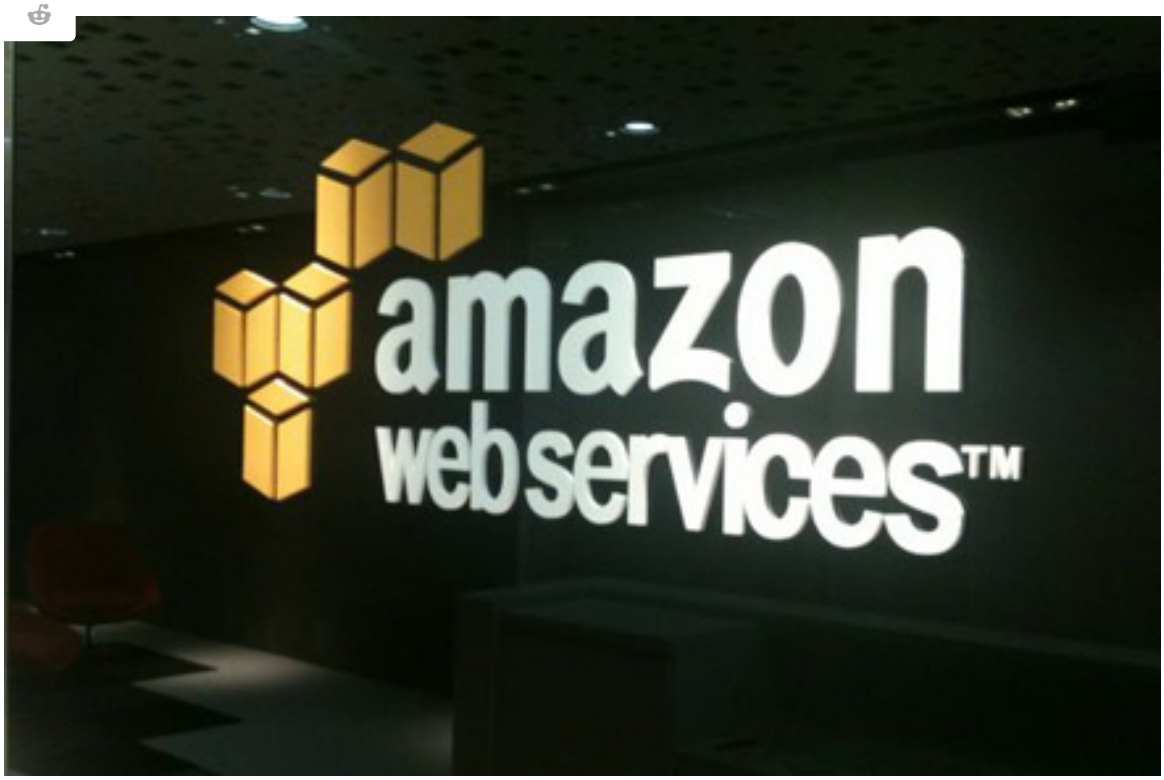
nazon Web Services Faces Steep :curity Challenges in the nterprise

Casaretto | Jan 30, 2013 | CLOUD, Featured Articles, NEWS | 7 comments



As **Amazon's Web Services makes its move into the enterprise**, one of the biggest obstacles they face will be in the world of security. The stakes are huge in a mission-critical enterprise environment, the elements of risk, security, and compliance have formed a significant barrier to public cloud adoption. Tactical, strategic, and security professionals throughout the industry are finding difficulties in making this switch. At root of these issues is the outright lack of control and visibility into a cloud provider's infrastructure; a deal-breaker in case after case because of security and compliance concerns. The amount of transparency that Amazon operates with requires a massive leap of faith that the typical enterprise cannot embrace – even legally in some cases. The **AWS Risk and Compliance whitepaper frames an arrangement that lays out a "shared responsibility" security structure**, in that AWS controls the physical aspects of the technology to the hypervisor, and all layers beyond that are on the customer.

> *"For the portion deployed into AWS, AWS controls the physical components of that technology. The customer owns and controls everything else, including control over connection points and transmissions."*

Top Stories

AWS Architecture

This right here is the Achille's heel of the AWS enterprise proposition. Within the nature of this cloud business is the oversubscription of physical assets, when it works it works well, when you go over that tipping point, not so well. For small businesses, despite requiring a bit of technological savvy to launch, AWS can provide a tremendous capex and even operating advantage, and for the developer crowd and others of the sort, the ability to spin up resources is a natural winning technology advantage- that market is well-established. However, the shared model can be the source of severe enterprise headaches where many answers are not easy, so I reached out to a number of enterprise industry professionals for their perspectives.

Even if AWS were to embrace some kind of limited visibility and control (however delegated) of the underlying architecture – it poses an untenable security and risk threat. AWS is in an interesting position based on how their systems are architected; the dynamics of multitenant services introduces several elevated risks. One such pain is the **"noisy neighbor" situation**, where a node becomes saturated with the computing demands of a co-habitating customer and it impacts your performance. We've recently seen a number of outages on Amazon services that have brought down scores of sites in a single outage.

Risk

When infrastructure is stacked high, a single piece can bring multiple systems down, thatis just a fact. Denver-based Summit Security Consultant and industry veteran Eddie Mize confirmed the elevated risk posture, adding that security could additionally be compromised by faulty or malicious API or other faults (and in some cases it could be Amazon executing this itself), meaning there is no existing way for compliance and security mechanisms to integrate with Amazon's services as they are. He shares:

> *"The cloud in various forms, and in any multitenant environment is **by nature, insecure**…In regards to the enterprise, it is my advice to proceed and pursue benefits in certain situations, but do so with caution and be strategically aware of risks, plan accordingly"*

Compliance and Regulations

With architecture is based on shared virtual servers, the difficulties in meeting compliance and security regulations for businesses that require this are many. AWS does not let customers do audits of its security. It has been reported that certain customers have been successful in getting insurance regulators into meetings with Amazon's security team. Large organizations will undoubtedly be staring at some challenges in the AWS environment. With limited flexibility on what constitutes security incidents, auditing, and required access, this flies in the face of the risk-averse and responsible enterprise and will continue to be a significant barrier to large enterprise adoption. Even in cases of dedicated, physical instances these AWS constructs still apply and require a leap of faith that a typical large organization may not take.

Streaming music on fire: Spotify increases users to 75m, 20m of them paid subscribers

HP fronts up $100M to settle Autonomy-related shareholder suit

Mesosphere's Data Center OS launches into general availability

Microsoft launches 1TB Xbox One and gives 500GB console a permanent price drop

Spotify raises $526m Series G on a $8.53b valuation to keep up the fight against Apple

Premium Research

Changing Mindsets from Magnetic Storage Tiering to Flash Data Sharing

- David Floyer

IT will sound like yesterday's news if it continues to advocate tiering, advocate putting the most important data on high performance storage, and declaring that less expensive lower performing storage is key and necessary. Today's flash reality is that a single compressed/de-duplicated

Working Through the Cloud

.

HP Enterprise Security Services leaders Andrzej Kawalec, Global CTO and Jeremy Ward, Offering Manager touched on this topic in a briefing this week. The group deals with many customers and has witnessed hesitation and delays in cloud adoption based on these very concerns. They confirm that in such cases, many shops are going to alternatives such as managed services. It gives them greater oversight into security controls, management,forensics and more practical tasks in achieving compliance goals. They definitely see a need for AWS and partners to evolve in terms of technology and process, bridging significant gaps, and provide a better product, adding:

> *"Without at least joint crisis planning and management however, these concerns will continue"*

Cloud Alternatives – Better for Enterprise?

.

Further evidence of the enterprise gravitating away from AWS emerged in a conversation with Brady Ranum, Vice President of Sales Engineering at **ViaWest, a super-regional managed services provider**. While ViaWest is not a direct competitor to AWS, they do see what insiders call "Amazon graduates" – meaning clients have found they are running into limitations when it comes to their enterprise needs on AWS. The concerns being heard should sound familiar and include compliance, security, rising costs, 'noisy neighbor', just to name a few – and these issues bring them to the world of managed services. In some cases customers are locked in to the platform, requiring a significant exit strategy to detach from the service. One client apparently discovered existing personal identifiable information, or ***"PII"*** throughout the AWS environment and had to launch a
two-year plan to clean it all up.

> *"We see are seeing more and more clients that have looked at pure cloud solutions and realized that managed services is the way to go for their needs across the board. Even in cost savings, in that once they need to scale elsewhere, the costs quickly become prohibitive, and that's where we step in"*

Time for New, Better Security

.

At the end of the day, the obstacle that causes the most concern is security. An enterprise that is looking to bring their own security simply does not have a lot of options in doing so. Few true software based security solutions actually exist out there, but one of the leaders in cloud security is **Alert Logic**. I reached out to Misha Govshteyn, Founder and VP of Emerging Products; he also confirmed a number of these concerns and shared a number of thoughts on this.

> *"Applications are moving out of the enterprise, but security largely hasn't made a broad move there yet."*

Govshteyn sees a security industry that needs to rebuild products from the ground up to answer these rapidly more sophisticated cloud needs. This requires a big shift in thinking, before things like DLP and log management in the cloud can become a reality. The responsibility is shared between the security provider and the cloud provider, but it's something that needs to be ingrained at every possible level with customers involved, vocal, and ready to make the move. It was this kind of synergy that led Alert
Logic to the industry's only network-based cloud IDS, a problem that seemed unsolvable

physical version of data must be shared between as many different applications as possible, because the incremental cost of creating and sharing another copy is close to zero.

Systems of Intelligence: The Next Generation of Enterprise Applications built on Big Data

- George Gilbert

Systems of Intelligence will power the next generation of enterprise applications built on big data. Line of business executives charged with digital transformation must understand the dynamics of Systems of Intelligence well-enough to be effective sponsors of new systems. IT executives must be effective partners and understand how to build Systems of Intelligence on top of Systems of Record. They will also need to understand how to build a radically new infrastructure to support these systems.

OpenStack as the Integration Engine for Modern Infrastructure

- Stuart Miniman

OpenStack is now positioned as an Integration Engine - not the entire stack, but like Linux, could grow into a critical component of IT over the next decade. This article examines the real state of OpenStack after the Kilo release and 2015 OpenStack Summit in Vancouver.

Top Ten Reasons why CIOs Should Migrate to All-flash Datacenters by 2016

- David Floyer

Wikibon believes CIOs should put the highest priority in developing an all-flash datacenter strategy, and implement it so that all storage acquired and deployed is 100% all-flash by 2016. The key short-term focus for CIOs is to ensure that data sharing is optimized, and that IT organization and objectives support and drive

just 3 years ago. He also reports that an emerging strategic dynamic exists where business owners have gone outside of IT in an effort to get faster delivery and are utilizing these cloud services. In essence, these organizations are becoming hybrid architectures and this is happening in instances where business owners can prove the security is tight, IT response was not as quick, and the business agrees the risk is low. This is where strategic consideration of cloud-based services steps in, with the advent of this new perimeter architecture, there are possible ways based on application and information in the cloud to work and still satisfy several compliance regulations.

Still, Amazon will face a number of enterprise challenges in being competitive ins such fields such as pricing, security, compliance, and risk. The outages haven't helped, so until some successes come in transforming these deficiencies, the industry will probably be somewhat averse to embracing these services wholesale. Security, risk, and compliance are especially significant in the enterprise, it goes way beyond a mere cost play. Cloud-based services should be regarded as a strategic tool to gain certain advantages, but for a continued bevy of unmet enterprise requirements, they should be carefully reviewed and planned for before going mission-critical. This is something CIOs and people across the spectrum are looking at and will be watching as Amazon makes its move for large business.

John Casaretto

SiliconANGLE's CyberSecurity Editor - Have a story tip or feedback? **Please reach out to me**!

Security is as critical as ever and our mission is to uncover those stories that will help our industry be more secure.

7 Comments

Day1Solutions on January 30, 2013 at 10:47 pm

Hi Jeff, what are your thoughts on bridging the enterprise gaps with solutions like NetApp Private Storage for AWS? https://communities.netapp.com/community/netapp-blogs/about-data-storage/blog/2013/01/15/why-netapp-storage-for-amazon-web-services-makes-sense

Our customers feel this address most of their security concerns in the cloud, especially when adding isolation like Direct Connect, VPC, and even Dedicated Instances if necessary. IAM is another area of concern, but there are great 3rd parties that augment AWS to further harden access. Low hanging fruit like long term archive or test/dev quickly move to production conversations as enterprise customers are better educated and experienced in what's possible with AWS.
To your point about shared security model, yes that's left up to the customer, but for companies like ours it creates a great opportunity to help our enterprise clients implement this properly and establish a long term relationship.

-Luis

more if you're interested http://day1solutions.com/netapp

Day1Solutions on January 30, 2013 at 10:48 pm

Hi John,
What are your thoughts on bridging the enterprise gaps with solutions like NetApp Private Storage for AWS? https://communities.netapp.com/community/netapp-blogs/about-data-storage/blog/2013/01/15/why-netapp-storage-for-amazon-web-services-makes-sense

Our customers feel this address most of their security concerns in the cloud, especially when adding isolation like Direct Connect, VPC, and even Dedicated Instances if necessary. IAM is another area of concern, but there are great 3rd parties

increases in data sharing. The key long-term focus is to release the potential of the best and brightest in the organization to imagine an organization supported by applications without data limits.

Cloud Foundry Guides Enterprise IT Towards Cloud Native Applications

- Stuart Miniman

The emerging PaaS platforms (Cloud Foundry, Heroku, OpenShift, Docker) are all evolving to capture the mindshare of developers. While the PaaS battles are still in early days, Cloud Foundry is emerging as a leading open source platform and ecosystem to build and deploy the new Cloud Native applications that are driving these economic changes via software. But this Platform-as-a-Service (PaaS) model requires changes to technology, skills (people) and internal IT processes. This means enterprises need to become familiar with this development and operational model to best understand how they can accelerate using Cloud Native applications to give themselves a business differentiation.

that augment AWS to further harden access. Low hanging fruit like long term archive or test/dev quickly move to production conversations as enterprise customers are better educated and experienced in what's possible with AWS.
To your point about shared security model, yes that's left up to the customer, but for companies like ours it creates a great opportunity to help our enterprise clients implement this properly and establish a long term relationship.

-Luis

more if you're interested http://day1solutions.com/netapp

jgershater on January 31, 2013 at 8:50 am

For shared responsibility, I wrote about this earlier this year
http://cloud.trendmicro.com/security-in-the-cloud-is-a-shared-responsibility/
and accompanying demo video
http://www.youtube.com/watch?v=PbjKBTQLCBw&feature=share&list=PL92FE08CA388779B7&fmt=22

scottherson on January 31, 2013 at 2:21 pm

Other IAAS firms can be considered for their security advantage. Joyent Cloud for example (Disclosure, I work there). From http://www.joyent.com — "Joyent is the only solution in the industry to deploy Zones, a technology that acts as an additional, "steel-wall" that prevents neighboring tenants from attacking other occupants. Zones provide the best internal security in a multi-tenant environment and offer an additional level of confidence over legacy cloud architectures".

John Casaretto on February 1, 2013 at 10:51 pm

@jgershater Let's talk – email sent

John Casaretto on February 1, 2013 at 10:56 pm

@Day1Solutions Luis – thanks for the links – Can you look me up I'd like to discuss

zoharalon on February 5, 2013 at 5:36 am

The main challenge that we see @Dome9 is how can traditional IT evaluate and procure security products and solutions for an environment they are being forced to support, both from Devs pushing up (or avoiding IT altogether) and CIO pushing down.

The fact that AWS is constantly evolving and adding more and more, helps scare enterprise IT, and from our experience, creates even more opportunity for security products.
We offer a complete Security Management and Automation for EC2 and VPC that offers multi-user/admin granular policies, auditing (that AWS still doesn't offer) , policy reporting and compliance, and a cool alternative to client VPN that is a very big IT challenge in the cloud.

Cloud, and AWS specifically, challenges traditional Enterprise IT thinking in many ways, and the role of the IT security industry is to offer tools that Ent IT can easily adopt (i.e. have reasonable UI, reporting, professional services), and that would allow for soft landing into understanding, evaluating and ultimately solving their enterprise cloud security challenges.