Analyzing Security in Cloud Services

An Annotated Bibliography

Jeff Miller

Graduate

School of Information Systems and Applied Technology

Southern Illinois University

Carbondale, IL

Southern Illinois University

November 22nd, 2020

Cloud Delivery Models Security: There are three cloud delivery models including SaaS, PaaS, and IaaS. The purpose of this research is to do a comparative study the security of the three cloud computing delivery models. The focus of your research should be on the application development for each, the security technologies/mechanisms including authentication, authorization, access control, etc. and reliability of each one of them.

Cloud Security

IAAS Platform

Three cornerstones of security that you need or your organization is to as platforms now is tools like AWS Azure GCP they provide a lot of scalability and efficiency to enterprises but you have to make sure that you do what's necessary to secure them so when you're using an iOS platform there are three things you need to consider one data at rest now these platforms they a lot of data inside of Buckets and all that kind of fun stuff and you have to make sure you can detect sensitive data patterns at rest and input controls around that data #2 custom applications custom master things that your organization builds 'cause it knows exactly the type of tool that it wants to use and you have to make sure you're securing access to these applications as your employees are you finally SSPL CSPM stands for cloud security posture management and this entails scanning eyes instances for misconfigurations that are associated with established benchmarks of good news is keasbey's cloud access security brokers

I folks and welcome to our whiteboard video on ensuring cloud security in eyass pass and sass environments over the next few minutes I'll be walking you through how to manage some of your information security risks while leveraging the benefits of the cloud today well it should come as no surprise cloud adoption has never been higher to put specific numbers to it but you know trans report from 2018 had 72% of respondents say that they've adopted the cloud what's amazing is that this is up from only 48% two years earlier in 2016 unfortunately security remains one of the largest hurdles your organization is moving to the cloud this is one of the reasons infotech decided to create this research to help shed some light on security and help you overcome that hurdle now finding a trusted cloud service provider is no easy task to help you with this info tech has come up with a custom cloud security framework called the cagey approach which stands for completeness auditability governability an interoperability of a vendor when assessing a vendor the first thing you want to look at is how completely they cover your security requirements therefore you need to know what your security requirements are before you even approach the vendor the more requirements they are able to meet the safer we can consider that cloud to be next you want to look at the auditability of the bend what kind of questions are they going to be willing to answer about their security practices what kind of security certifications do they hold the more questions they're willing to answer the more auditable that environment is going to be considered to be the next logical step is to look at the transparency of the cloud specific policies and procedures need to be in place to ensure govern ability in the cloud so the more policies and procedures that vendor is willing to work with you on the more transparent we're going to be able to consider that cloud be and finally we want to look at the interoperability of the cloud where does that cloud service need to integrate with your environment and what kind of security needs to exist there the better that Able to integrate into your environment the more portable that cloud can be considered now the cagey approach is just one step in the process this research also helps you build slay documents and teaches you how to negotiate with vendors it helps you build an implementation road map and a communication plan for cloud security and finally it helps you build a governance program that allows you to ensure security on an ongoing basis that's it for a

quick overview service is able to integrate into your environment the more portable that cloud can be considered now the cagey approach is just one step in the process this research also helps you build SLA documents and teaches you how to negotiate with vendors it helps you build an implementation road map.

Structure in Azure with virtual machines there's so many options available for cloud computing that you really can propel your business faster and further if you just know about and embrace some of the new modern options that allow you to get more compute done in faster periods of time and allow your business to get things done faster without you having to manage so much of the infrastructure maybe we should talk about that a little bit wait a second that's a pizza guy one second Hey Dean app here welcome to the show that helps Azure administrators to know option while master the Microsoft cloud you know just before I get into this pizza here I would I think he called computing I think pizza might be a great analogy to try to help understand the different options that are available think about it for a second when you make a pizza at home you're in complete control of it right you make the dough and you put on the sauce and you select the right cheese is in the right toppings and you're responsible for cooking it and when you're done you are going to cut it and serve it up and hey it's great and it's built exactly the way you want it and I think that's a great way of explaining infrastructure we have to manage on premises right and then we start thinking about options that are in the cloud I think of a you know taking big pizza where you don't have to worry about the cross store the ingredients that's all taken care of for you and then you just have to go to the freezer and pick it out and bring it home and cook it up you still responsible for the electricity in the oven and making sure that's all there and cutting it up and serving it up of course we could just easily pick up the phone and in which case you didn't have to think about any of that stuff right you make the order but they take care of all the ingredients they take care of cooking it they take care of electricity they deliver it to you and you just got to enjoy it and then of course if I wanted to I keep going on really good pizza place myself and just go in dine in eat there and then take care of it I think

of making pizza at home is like your on premises infrastructure and those take and bake pizzas from the frozen food aisle that's like your infrastructure as a service and delivery that is platform as a service that's got some things you're still responsible for but ultimately most taken care of and then of course the piece that is false it's having that sass having that pizza place you can go into and it's all taken

For you and what's interesting is we can kind of correlate that to lots of different types of solutions available in Azure let's use SQL as a good example you can easily go rack stack and cable infrastructure and have that run in on premises for you you are responsible for installing windows and you're responsible for setting up SQL Server and getting the licenses and taking care of all that and that's how we've always done it of course these days you can go into the Azure marketplace and you can buy the virtual machine compute you want and it could be preinstalled with Windows Server and with the SQL Server you want Microsoft even goes so far as to make it available so if you wanted to cluster SQL infrastructure you can buy that which will give you a full set of VMS properly configured for their default configuration but if you don't want to manage that you know it's possible when you have infrastructure that you have to take care of that that may not be your strong suit that may not be your expertise so why worry about that there's options in the platform as a service where you can use something like Azure SQL database where you don't have to worry about the infrastructure at all you don't have to worry about its configuration you just host your data in the cloud using SQL database now maybe you have a application that isn't capable of using Azure SQL database yet and that exists well then you have things like SQL database managed instances which is literally Microsoft taking advantage of their expertise and they're administering SQL Server for you in the cloud or you can go all the way up to modernizing on new data stores that you haven't thought about before like Azure SQL data warehouse or even moving to a no SQL solution like cosmos DB like there's so many different options that allows you to have the right flexibility and exchange cost for savings in time and effort from administrator point of view and I think that's one of those things that's missing today is that we don't always look at those options available

to us we're so used to maintaining and managing that infrastructure that sometimes we have Blinders on and we're not look Kind of stuff but what I find interesting is that I can leverage Microsoft's expertise and take advantage of some of those services especially for the platform as a service so that the common stuff they take care of it so then our engineers focusing on the data layer can leverage the cloud technology the way it's meant to be but it's more than just data because we're modernizing applications these days so it's not always just your typical client server application you now can take advantage of event driven modern applications that are built out in many ways even in serverless technology you know it's not just about running compute through an Azure virtual machine you can take advantage of using modern web apps on containerization things like Azure container instances giving you just in time compute when you need it to only do execution so as an example for me at work we have a bunch of reports that need to get generated every single week and instead of having to worry about scaling that up all the time we just use ACI we use Azure container instances we built out containers specifically to do the jobs we needed to do and then we use a scheduler through an Azure function that will load up that container execute do the work store that securely in Azure blob storage and then give us the ability to alert us that the reports are ready and all of that becomes a more modern way of taking advantage of compute in a way that makes more sense for us as we've been growing we've been able to scale that out so that we can get that same amount of compute done in a shorter period of time and that's because we take advantage of things like Azure functions and events and the event hub to be able to drive that stuff together and these are all just different parts of where compute works out so

EA GUIDING PRINCIPALS 1

- Define protections that enable trust in the cloud
- develop cross platform capabilities and patterns for proprietary and open source providers

- will facilitate trusted an efficient access, administration, an resiliency to the customer slash consumer
- provide direct to secure information that is protected by regulations
- the architecture must facilitate proper and efficient identification, authentication, authorization, administration, an audio ability
- centralized security policy maintenance operation comma and

EA GUIDING PRINCIPALS 2

- Access to information must be secure yet still easy to obtain
- delegate or federate access control where appropriate
- must be easy to adopt and consume, supporting the design of security patterns
- the architecture must be elastic, flexible, an resilient, supporting multi tenant, multi landlord platforms
- the architecture must address an support multiple levels of protection, including network, operating system, and application security needs

Building security at every layer

- every cloud architecture is composed of unique layers that can be coupled an integrated or not
- to some degree, each layer must be self-defending
- the new cloud infrastructure and application stack have a number of components
- each layer needs some sort of security integrated an applied to build a sound defense in depth architecture for the cloud

- depending on the layer some will be applied in house others in the CSP environment

Building security at every layer 2

Stack layer followed by controls

application logic plus presentation layer WAF, I am, scans slash penetration tests

operating systems layer configuration, vulnerability scanning, backups, user slash privilege management data encryption, backups, DLP

network layer access controls, firewalls, routing, DDoS defense

Hypervisor layer configuration, access controls, user slash privilege management

Building security at every layer 3

Given the nature of the cloud, it changes much more dynamically than ever before

for this reason all security measures should ideally be embedded

BY: defining security and code internally

including security configuration parameters in VM definitions

automating security process is an activities

building continuous monitored environments

And that's something I'll talk about here momentarily as well identity management is really becoming the linchpin of cloud security in a lot of ways but if any of you have ever spent anytime designing some of the policies especially in places like KWS it is incredibly easy to screw it up I know this because I have screwed it up so if I get it right one time and I make sure it works appropriately

and I you know really work to get those least privilege aspects in place I really don't want to have to do it again so do it once invoke it whenever you need it so that's the idea of components and it really comes into this notion of centralization and centralized control that gosh drive 4 if we're ever going to succeed in the world of cloud security there's no way we're going to get there without really sort of embracing this concept and I'll take this even further and put it into what I call the multi cloud problem maybe it's not a problem a lot of times for security professionals it feels like a problem because the minute you guys get I got this you know I've got I've looked at all their documentation and certification from those guys somewhere in your house Microsoft sales people are taking your folks to lunch and guess what that's how it begins and the next thing you know you've got some stuff in Azure and then all of a sudden you're going well how did this happen and then the next thing you know Google is a part of the conversation again this is how it begins but that's really the nature of Business Today if you're completely invested wholly in one cloud environment today don't get too used to that there's a lot of business drivers that are pushing people to adopt multiple cloud providers and if you're really thinking about a tool for a service or a specific control that is wholly centric to that one provider then you're going to find yourself locked in an incompatibility situation very very quickly take step back think about components but think about components that can ideally be adopted or adapted to more than one cloud as an architectural principle and design model and what that means is that if you're saying hey we are really good right now with Microsoft's Azure resource manager templates or we're really good right now with Amazon's cloud formation like I got it I know the syntax I got everything designed the minute you get all your cloud formation stuff lined up and somebody spins you out into Azure and you got workloads there now you've got to go back and say alright how do i adapt this to work over here and there might be But when it happens and #2 for potentially state that is no longer failing and so there's this entire idea out there that I'm sure some of you are at least somewhat familiar with today it's called chaos engineering and it started with some of the folks

we heard of at least a few of them in the past couple of years but nonetheless there are plenty of them out there this is another concept that security people have really had to adapt to and it's

designing for elasticity – May not seem like it is directly linked to security but it is and must be considered in the design of secure architecture.

One of clouds for most benefits is the ability to rapidly scale up and down as needed for business volume an requirements. Designing elasticity into your models means considering the following, vertical or horoscope scaling vertical or horizontal scaling what thresholds are appropriate for scaling up and down? How will inventory management adjust to system volume changes?

images new systems or spawn from where new systems will operate network locale host based security plus licensing

Storage Explorer options

there are many types of storage available in the cloud

understand each type and which are best suited for your deployment

each has its own security options available too

revisit data classification and data security policy before planning storage security design

performance matters too of course

Secure design in a “feedback loop”

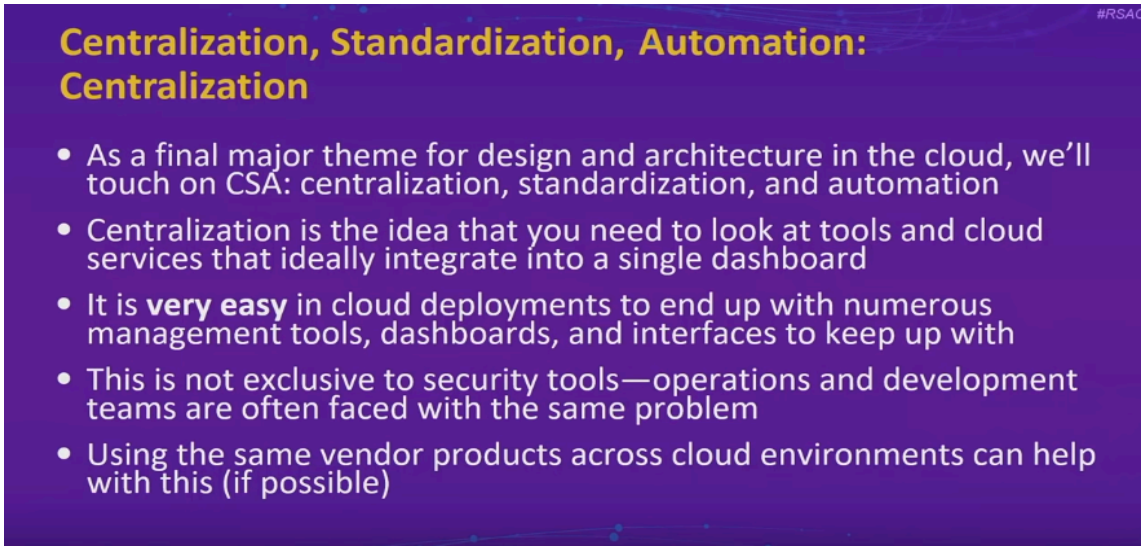
Logging

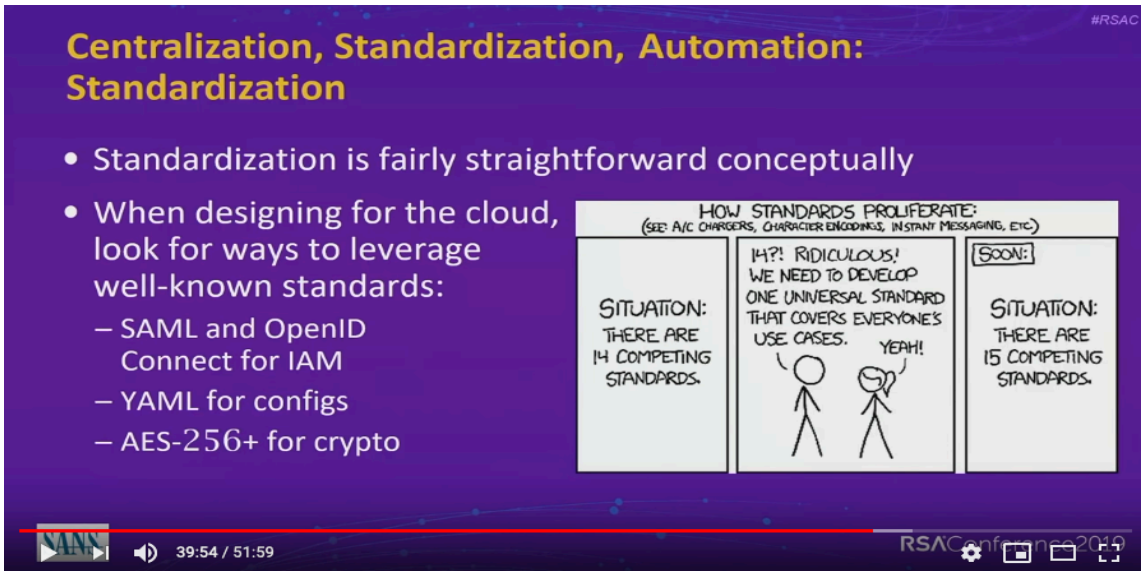
Your primary source of feedback is logs enable logging wherever you can within the cloud environment as a whole OS types for network platforms for all identity and access management activity for all interconnected services in their activity be sure to secure access to the logs as well

You could use one of many numerous alerting and monitoring mechanisms in major cloud environment the learning methods are becoming more popular and many services offer monitoring in a dashboard that aggregates monitoring like activity logs, diagnostic logs, and metrics.

DFS Google app If you want to make the primary adfs what do you suggest to really go for that next step in ensuring that no failover well it's it's a great question you know and basically saying how do you I mean you're talking bout adfs meaning your own internal Active Directory you are synchronizing out to various environments number one make sure your internal directory services are always available right because I mean obviously if you're still linking back to your on premises and that's a connectivity scenario so you're federating but how were you federating are using a third party provider that's in the middle of that are you synchronizing to active Active Directory and Azure that's a that's a pretty big question to try to answer without having a look at your architecture itself but I'd say you know if I had to gauge it at some point and it may not be now you're probably going to ask yourself are we going to be better off if we just shift the primary into the cloud versus doing it on premise I'm not going to answer that question for you but Microsoft will probably suck you into that black hole at some point anyway just wait give it time so I'll have to talk to you offline about that too Data ownership model but if you look at the roles and responsibilities data and governance is always the owner or consumer of the service So what kind of checks and balances additional checks and balances would you take into account for that it's a good question to big one yes it is I mean yeah you know I guess we're out of time but I will tell you it comes down to #1 asking the right questions of the cloud providers you still gotta trust them to some degree and you got to read those invigorating sot 2 reports that you know you love but the

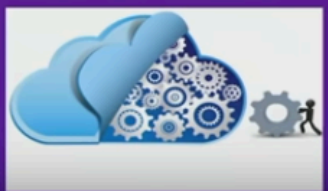
data is yours though it is yours but at the same time you know you've got to have some geographic centricity that those guys are guaranteeing which is typically a contractual scenario I mean you're not tracking your own data of some sort of you know Geo tagging or something so you've got to be able to ascertain that these providers are willing to contractually guarantee that which means that if you're in multiple different regions you're probably going to be limited to a very short list of providers in the 1st place but it's another big question I don't know that I answered it well but it's a tough one and I think we're out of gas so thank you very much for comin





Centralization, Standardization, Automation: Automation

- Automation is the core idea behind DevOps, and DevSecOps by extension
- Manual efforts in the cloud are doomed to fail in many cases, as the environment changes rapidly
- Security teams should explore ways to automate their security controls and feedback loops whenever possible
- Scripting and orchestration tools can help!

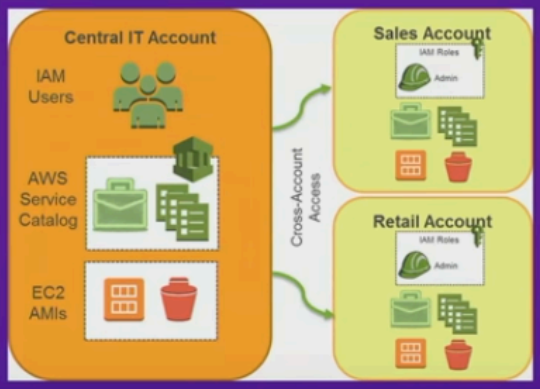


Managing the Cloud "Blast Radius"

- One of the core security concepts in the world of DevOps and cloud computing is the "blast radius"
- The blast radius is the amount of damage that could be caused if something goes wrong
  - An account or server gets hacked
  - A component fails
- Design your security model in such a way that you limit the damage any one issue could cause

Multiple Accounts for Limiting Blast Radius

- One cloud security strategy that has emerged in recent years is the use of multiple accounts for limiting blast radius
- Accounts can be created for:
  - Developers
  - Business units
  - Operations
  - Security
- These can then be allowed access to objects and assets in other accounts as needed
- AWS has a service called "Landing Zone" to help set this up
  - A newer service called "Control Tower" is also now available to implement this



Applying This To Your Organization

- Next week you should:
  - Determine your level of overall architecture maturity
- In the first three months following this presentation you should:
  - Ensure you look into multi-account or subscription architectures
  - Ensure centralized, infrastructure-as-code deployments are planned
- Within six months you should:
  - Have a streamlined, central deployment incorporating DevSecOps principles
  - Ensure all feedback loop and storage controls are optimized