Executing an Efficient Cloud Security Strategy

15 Cybersecurity Experts on
Smarter Security in the Cloud

Introduction

Cloud computing is still on its meteoric rise, with a projected market share of $285.3 billion by the end of 2025[1]. It's quickly becoming the norm for organizations to base their operations either partially or completely in the cloud, thanks to motivations like cost savings, elasticity and improved productivity.

However, organizations often don't have the cloud cybersecurity education and training to keep up with the rate of cloud adoption and its associated security responsibilities. With issues from open S3 buckets to a lack of identity access management, how do large organizations implement an efficient strategy and find the right cloud security tools?

To try and answer that, we asked a range of cloud security experts to share their thoughts on some of the key cloud security challenges and provide advice on how organizations can implement a cloud strategy that will keep them secure.

[1] https://www.bloomberg.com/press-releases/2019-10-29/cloud-computing-market-share-is-estimated-to-reach-us-285-3-billion-by-the-end-of-2025-with-a-cagr-of-29-2-valuates

The advice I would give for people operating in the cloud who are having problems with an effective security strategy is this: You need a complete view of everything you have, and you need to have one identity system.

The other thing you need is visibility. You need to be able to see what's on-prem, what's in Cloud A and what's in Cloud B. Having complete visibility over everything allows you to monitor it, respond to threats, etc.

If you can't see everything you can't possibly protect it. This is my number one advice for people operating in the cloud who are having trouble making a good security structure around it.

Tanya Janca
Application Security and Cloud Security Consultant
@shehackspurple

So, you're joining the stampede to the cloud but are struggling not to be trampled. This phase is about survival, not elegance. Use your limited resources strategically. I would recommend three broad courses of action:

1. **Triage:** What are the key assets moving into the cloud that the company can't afford to lose? Give them the resources first. Let the low-value asset owners know that they are at risk.
2. **Focus on ROI:** The first five of the 20 CIS Controls block 85 percent of all attacks. The other 15 controls give you only 12 percent more coverage. Spend your time on controls that give you return.
3. **Recruit the masses:** According to IBM, two-thirds of records lost were the result of human error, not state-sponsored hacking. You won't stop issues like misconfigurations via education, but you will slow the leak.

It would also be useful to create a five-minute video that describes the top three cloud configuration errors in business manager language (i.e. small words, short sentences, color pictures). You can then point business managers toward self-help data for the technical detail.

Stephen Wood
Product Manager,
Tripwire
@TripwireInc

In my experience, organizations that move to a cloud environment are often challenged when it comes to achieving a strong cloud security management strategy. That's because they're still in the mindset of the on-prem local server management paradigms, and they look to the cloud as an opportunity to simplify when they make a decision to change.

While allowing a cloud infrastructure provider to take on a huge chunk of your IT team does allow you to simplify your technical security strategy, I find that a key challenge these organizations have is shifting to an approach that focuses on user behavior management.

My advice is therefore twofold. First, before moving to the cloud, it's a good idea to reassess your data management strategy. Does your organization truly understand where your sensitive data sits? How does it flow inside your organization and your cloud infrastructure? You should map out your locations, users, posts, etc. and identify where the data moves around. From there, you can potentially identify areas of weakness or lack of compliance, and plan around that with the right products, processes and policies.

Ben Schmerler
Director of Strategic Operations, DP Solutions
@dpsolutions_md

My other piece of advice is to make sure you have a comprehensive strategy to train users on security awareness, especially as it pertains to social engineering, phishing and other attacks. They're less about technology and more about users. When things shifted to the cloud, the cyber threats shifted towards exploiting users in a major way.

The solutions to your security challenges in the cloud will vary based on what you do, so having consistent assessment of your security solutions and train your people will be the keys to your success.

A great start for any organization wondering how to create an efficient cloud security strategy would be to tap into the wealth of free and vendor-agonistic information offered by the Cloud Security Alliance (CSA).

The CSA is a not-for-profit, collaborative organization with over 80,000 members and practitioners offering a wide range of industry expertise. Its mission is to "promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing."

One of the best documents to begin with is the CSA's Security Guidance for Critical Areas of Focus in Cloud Computing. This guide provides a great overview of the cloud itself and of essential high-level security considerations.

Then take a look at their Cloud Controls Matrix (CCM), a baseline set of security controls to help enterprises assess the risks associated with a cloud computing provider.

For those who wish to take matters more seriously and seek professional training and certification, the CSA has also partnered with (ISC)² to establish the CCSP (Certified Cloud Security Professional). Effectively, CISSP applied to the cloud!

Angus Macrae
Head of Cyber Security
@amacsia

> The key to overcoming the challenges of implementing information security in the cloud is not to overcomplicate the problem. It's really easy to get distracted by the technology and the newness of that technology, but the reality is that the controls that you need to implement in your cloud environment aren't really that new.
>
> You still need visibility into what assets are there. You still need to be able to assess how they're configured and ensure that that configuration stays the same. You still need to be able to find and address vulnerabilities in that environment, and you still need to be able to detect changes when they occur so that you can make sure those changes are authorized.

Tim Erlin
VP, Product Management and Strategy, Tripwire
@terlin

There are two key challenges we see organizations struggling with: crafting policy and enforcing policy.

Both are challenging because consistency is a key constraint on both. Because there can be technical challenges to consistently creating and enforcing policies, organizations end up with mismatched security capabilities. They basically implement what they can in each environment even though it may be different from the desired state.

This usually happens because orgs adopt systems and services in the cloud that are different from what they use on-premises. Alternatively, they might be forced to adopt different systems and services across cloud providers.

One way that organizations can overcome this challenge is to try to use the same systems/services across cloud environments. That often means finding a third-party provider that supports all desired cloud environments and standardizing on the system/service for security functions. This enables organizations to turn policy into enforcement consistently, and it has the benefit of using existing expertise with the system/service in multiple areas.

Lori MacVittie
Principal Technical Evangelist, Office of the CTO, F5 Networks
@lmacvittie

> I believe an important aspect for developing your cloud security solution is to consider how your in-house skills and processes work. If your team is already comfortable using a SIEM as a “single pane of glass” for all your security cases, make sure your cloud solution is able to connect and play well with your log management tool and your team’s response processes.
>
> If you are taking your existing security tools and expanding them to cover the cloud, you should also start thinking about how you are going to configure and maintain these tools so they cover your new cloud services and whether your existing on-prem infrastructure and processes are well placed to handle cloud concepts like elasticity—like making sure you can scan on arrival so you don’t get gaps in your monitoring developing over time.

Chris Hudson
Customer Services Consultant, Tripwire
@askjarv

In a corporate context, I want to flag typical pitfalls in due diligence and ongoing governance. Starting with a control wish list, in the form of a questionnaire lifted directly from your internal security policy, is a waste of time. Vendors make profits because everyone gets a similar service, and there is a limit to what they can or will change—even if you don't like it.

Critically, you need to confirm how they will give you visibility of continuous controls relevant to your SaaS, IaaS, PaaS or hybrid supply, e.g. vulnerability management, security event management, information and physical asset management or access management. Will they allow you to regularly audit other controls? Or if audits are a non-starter, will they evidence both adequate design and effective operation via a third-party audit?

If what they will share isn't enough to comfort you and they can't or won't change, then it's a risk tolerance decision. Are they the right vendor for you? Someone senior enough to make that call needs to document their decision.

The other thing that's utterly crucial to iron out is demarcation. Who are the go-to people on your side and their side? Will they stay in-post for long? (Vendors often have a habit of rapidly rotating staff.) How responsive can you rely on them to be? Where does your

Sarah Clarke
Data Protection & Privacy, BH Consulting
@trialbytruth

job finish and theirs start for threat and vulnerability management, incident response, data subject rights requests, access and identity management, downstream supplier or partner due diligence and integration or orchestration for the migration to cloud when things are added, connected or retired?

Some of that can get transferred to SLAs, especially incident response, when poor response times can lead to reputation damage and regulatory sanctions. More generally, you will be set up to fail if you don’t define these and other functional/non-functional requirements in time to do something about it. You should do this when the cloud idea is first floated, not the day before the service goes live.

Cloud has fundamentally changed how we use IT and consume IT services. Where data is, as well as how its transferred, stored and processed has changed with the utilization of cloud.

Let's talk about some of those challenges. First and foremost, the cat is out of the bag. We're not going back to the data center, and any resistance to that is going to be seen as a business inhibitor and will therefore not get much airtime.

I think that cloud has been adopted typically in silos because every employee has a credit card. That's a big problem because it doesn't allow the enterprise to have oversight across the board on how data is being processed and stored. I also think that "cloud" is pretty ambiguous as a term. Not all cloud service providers are created equal. AWS, Azure and GCP are pretty rock-solid, but 80 percent of the cloud we consume is not with them but with the mom-and-pop SaaS offerings around the world. Of course, those SaaS are living off of AWS, but we don't have a contract with AWS when we're using these services. We have a contract with the SaaS provider, and they habitually are terrible at security.

Alex Dow

CTO, Mirai Security

@mirai_sec

Security is fundamentally different in a software-defined world. For the cloud, this is a world of shared responsibility where half of the responsibility for security is ours and the other half is the service provider's. All of this gets very murky, and unfortunately, a lot of early adopters of cloud believe that the cloud service provider has almost all the responsibility. That's just not true.

Now let's switch tracks and talk a little bit about strategy. Understanding which cloud services have been adopted by your organization is the first step. We need to understand what data is being transferred, processed and/or stored in the cloud. Then we need to understand which security controls are in place to protect that data and who owns that. As discussed, there's a shared responsibility model. Part of the responsibility will be on you, and the other half will be on the cloud service provider. I guess I really shouldn't use the word "half" because it typically isn't an even-steven balance.

Next, and maybe this should have been the first part of the strategy, is the need to increase awareness to the business and the stakeholders. Cyber risk and privacy are very important these days, with privacy laws having pretty serious teeth. When we were storing the data in our own data center, we were really able to control how accessible it was. However, as we start moving our data into the cloud, we lose a lot of that control. Now if a cloud service provider does lose your data, you may be on the hook for a breach and possible privacy law violation and fine.

We need to enable, not inhibit, an internal team that may be using a SaaS that's insecure. We do want them to stop using it, but we need to bring a better solution for them first before we can start saying, "No, I'm taking tools away."

And lastly, look for the opportunity to review and refactor early adoptions in cloud, especially in the IaaS side of things. The lift and shift of bad from your data center into the cloud is likely going to come back and haunt you in the future, so it's best to look at an opportunity to start rebuilding some of those applications in the cloud and leveraging some next-generation, cloud-native technologies where security is baked in from the beginning.

When working to secure the cloud, the best thing to remember is that the cloud doesn't exist.

You're still talking about servers and services. The same people who leave their S3 buckets open would often never consider an open SMB share on the internet. Patching a cloud-based Linux host should have the same priority as one on your local network. At the end of the day, security is security, and whether you're talking about IT, OT, IoT, IIoT or the cloud, security fundamentals are the key.

I think that the challenge for a lot of people is the word "cloud." It becomes this new beast, and it creates confusion and brings challenges that don't need to exist. If you take a step back, all you need to consider is security basics. Once you master those, you are well on your way to success.

Tyler Reguly
Manager, Software Development, Tripwire
@treguly

Perhaps the biggest issue in cloud transformation is the stretch goals the business is trying to achieve—they are not realistic. As exciting and challenging as cloud is, I think the biggest problem is trying to reach for interstellar travel without visiting the inner planets and the moon. Just like NASA looking at the moon as a staging base for a Mars trip and one day beyond, business has to look at the art of the possible rather than a quantum leap forward.

Proof of concepts and making decisions on which systems can be replaced by SaaS offerings needs to be part of the strategy. Taking your legacy estate and lifting and shifting it to hosted platforms is not digital transformation, it's just putting the problems somewhere else and frequently making matters worse. Things go bad when you attempt to digitally transform without working with the IT teams and the security teams to figure out how to do it for the least cost, best security and with appropriate skills and tooling. All too frequently, the rush to the cloud falters due to unanticipated edge cases that prove to be business-critical—the program falters and the digital transformation becomes an expensive adventure without the benefits fully realized.

Ian Thornton-Trump
Head of Cyber Security, AMTrust International
@phat_hobbit

> Implementing an effective cloud security strategy is a difficult task. Most companies struggle to understand new concepts and thus try to migrate what they have on-premises to the cloud. My advice to those companies is: Identify the top three risks for your cloud.
>
> Learn how cloud-native companies such as Netflix are solving these issues and adapt their solutions to your cloud. Learn how these companies use automation to leverage the power of cloud computing and reduce any repetitive work previously performed by SOC analysts. Rinse and repeat. In order to implement the new security strategy, CISOs will need to hire more developers and fewer security experts.
>
> In most cases, developers can acquire security knowledge faster than security experts can learn how to code. Hire security experts to define the strategy and developers to write the infrastructure as code that will support it.

Andres Riancho
Application and Cloud Security Consultant
@andresriancho

How do you build an effective cloud security strategy? The first thing you need to do is build out your network access control and user access control policies, just like you would for any on-premises system. For cloud services, however, you're going to also need to include those specific cloud items.

Let's discuss access to instance metadata, for instance—something which is very specific for cloud instances. That's something you want to have restricted, and they need to have a policy that states specifically how you do that control and how you do that restriction.

Second, you need to socialize those policies. You need to let everybody within the IT world and perhaps even outside of that within your organization understand why this is so important. Without resorting to fear, uncertainty or doubt, you can point to all the cloud breaches that have been happening lately and say, "Hey, listen guys, this is real. This is what we need to protect our organization against and this is the reason why we have these policies in place."

Jeffrey Groman
Founder and Principal, Groman Consulting Group
@jeffrey_groman

The third thing that you need to do is make sure that you've got reference architectures for common cloud service deployments already built, and let the project teams just run with them. You'll want to reduce the friction that project teams need when they're trying to deploy a cloud service; if you do, you're going to have a huge win on your hands right there.

So, when you look at your cloud security challenges, avoid getting distracted by that shiny technology and focus on what matters. Those are the controls that you need to implement, and that's the one piece of advice I'd give: Focus on what matters.

When organizations move to the cloud, they immediately realize that many of the challenges they faced with on-premises systems are still faced in the cloud. Additionally, there are some new and very different challenges, especially around security and observability. The cloud providers' security operations interface with customers on a shared responsibility model. It is important for customers to understand where the lines of demarcation are.

For example, in an infrastructure-as-a-service model, the provider secures the facility and physical network, server and storage infrastructure. As a customer, it's still your responsibility to patch your servers and applications and control the flow of network traffic to your environment with firewalls, IDS/IDP, etc. In a Platform-as-a-Service model like AWS Lambda, the provider extends their responsibility to the server operating system, but the customer still needs to control access and secure the applications. As with securing on-premises services, securing services in the cloud is best achieved in layers. Understanding which layers you are responsible for is a key first step.

Joe Goldberg
Sr. Cloud and Infrastructure Practice Manager, CCSI
@devops_dad

> When organizations move to the cloud, they immediately realize that many of the challenges they faced with on-premises systems are still faced in the cloud. Additionally, there are some new and very different challenges, especially around security and observability. The cloud providers' security operations interface with customers on a shared responsibility model. It is important for customers to understand where the lines of demarcation are.
>
> For example, in an infrastructure-as-a-service model, the provider secures the facility and physical network, server and storage infrastructure. As a customer, it's still your responsibility to patch your servers and applications and control the flow of network traffic to your environment with firewalls, IDS/IDP, etc. In a Platform-as-a-Service model like AWS Lambda, the provider extends their responsibility to the server operating system, but the customer still needs to control access and secure the applications. As with securing on-premises services, securing services in the cloud is best achieved in layers. Understanding which layers you are responsible for is a key first step.

Frank Bennett
Deputy Chairman and Member of Governance Board, Cloud Industry Forum
@fboncloud

Extract from, "Thinking of Building a Digital Operating Model with the Microsoft Cloud Adoption Framework for Azure? Ask the Smart Questions."

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook