WHITE PAPER

Defining Your AWS Cloud Strategy In Five Phases

GUIDEPOINT
SECURITY

This paper examines key questions you should be able to answer when defining your cloud security strategy by delving into the five phases of cloud security architecture.

Identifying an effective cloud security architecture will depend on how your organization defines the cloud and the operational model chosen to build and manage your environment. Operational models include:

- ✓ CI/CD
- ✓ Lift-and-shift
- ✓ IaaS
- ✓ PaaS
- ✓ SaaS

In construction, building must begin with a firm foundation.

For a building to withstand sweltering temperatures, violent hurricanes, or freezing blizzards, all of the necessary steps and procedures must be followed to ensure the structure is strong enough to withstand such threats. If shortcuts are taken, the foundation may crack, leaving the entire structure vulnerable to damage.

Depending on the building size and style, the architectural requirements and construction steps will also vary.Therefore, architects and developers need to apply the right engineering and construction approaches to ensure the structural integrity of the building.

Like a residential or commercial building, successful cloud security architecture also begins with well-planned and high-quality foundation that is engineered to best fit the business.

Cloud isn't simply "cloud". Each major cloud service provider differs from each other. Additionally, if your path includes a multi-cloud deployment you'll need to identify a holistic architecture that fits within these differences, but also provides a uniform operations model.

Customers have utilized several different approaches for deploying into the public cloud for services such as compute, data analysis/science, storage, serverless applications, and more. In this paper, we'll explore the five phases associated with creating a cloud security architecture.

When it comes to cloud transformation, we've all heard that you should consider security BEFORE rather than after moving to the cloud.

Based on your cloud strategy and desired time to market for your application or replacement of your data center, there are several security challenges to resolve, such as determining whether to remain cloud native with respect to security controls or introduce third-party platforms. Additionally, one of the major obstacles we've observed is failing to apply "future proofing" to the security architecture. This is critical when we consider the speed at which cloud service providers enhance or release new services.

Based on a number of successful experiences, we've seen patterns and methodologies emerge which can be successfully executed when it comes to implementing cloud security.

The AWS application migration strategy is adaptable and works well with many customers.

Just like in the physical world, every cloud has a different shape and consequently adoption paths are not the same for everyone.

While the application migration approaches of many cloud service providers (CSPs) may work, often their steps can be an unstructured combination of both the tactical and strategic.

As multi-cloud becomes more of a common deployment pattern, organizations need an approach that is both tactical and strategic at the same time. Is that possible? We think so.

aws

AWS APPLICATION MIGRATION STRATEGY THE SIX R'S

1. Re-host
2. Re-platform
3. Re-factor/ Re-architect
4. Re-purchase
5. Retire
6. Retain

Cloud Logging, Encryption, Authorization

There are some issues to consider when it comes to the cloud in terms of logging, encryption, and authorization.

1. Cloud logging questions:
   - What do we log?
   - Where do we store our logs?
   - Do we encrypt the logs?
   - How do we interpret our logs?

1. Encryption questions:
   - Do we use a cloud native or third-party key management solution?
   - Who and what systems have access to data encryption keys and secrets?

2. Authorization questions:
   - How do we achieve and manage least privilege within a complicated entitlement ecosystem?

NOTE: Poor authorization can also present challenges that will need to be addressed.

Where to Start?

On occasion, security leaders have expressed concerns about cloud security, namely because they are unfamiliar with the cloud service provider's services. Sometimes what is needed is more discussion about the providers and their capabilities. There may also be instances when bringing in a third party makes sense.

The decision will depend on the strategy you have already developed and what makes the most sense for your business needs.

Once you've made a decision (or be forced into it because of an unexpected event such as a global pandemic) to adopt the cloud, security should be a major priority before you implement anything. If you have already deployed cloud resources, you should ensure you maximize all options to improve security. This may include leveraging both cloud-native and third-party platforms.

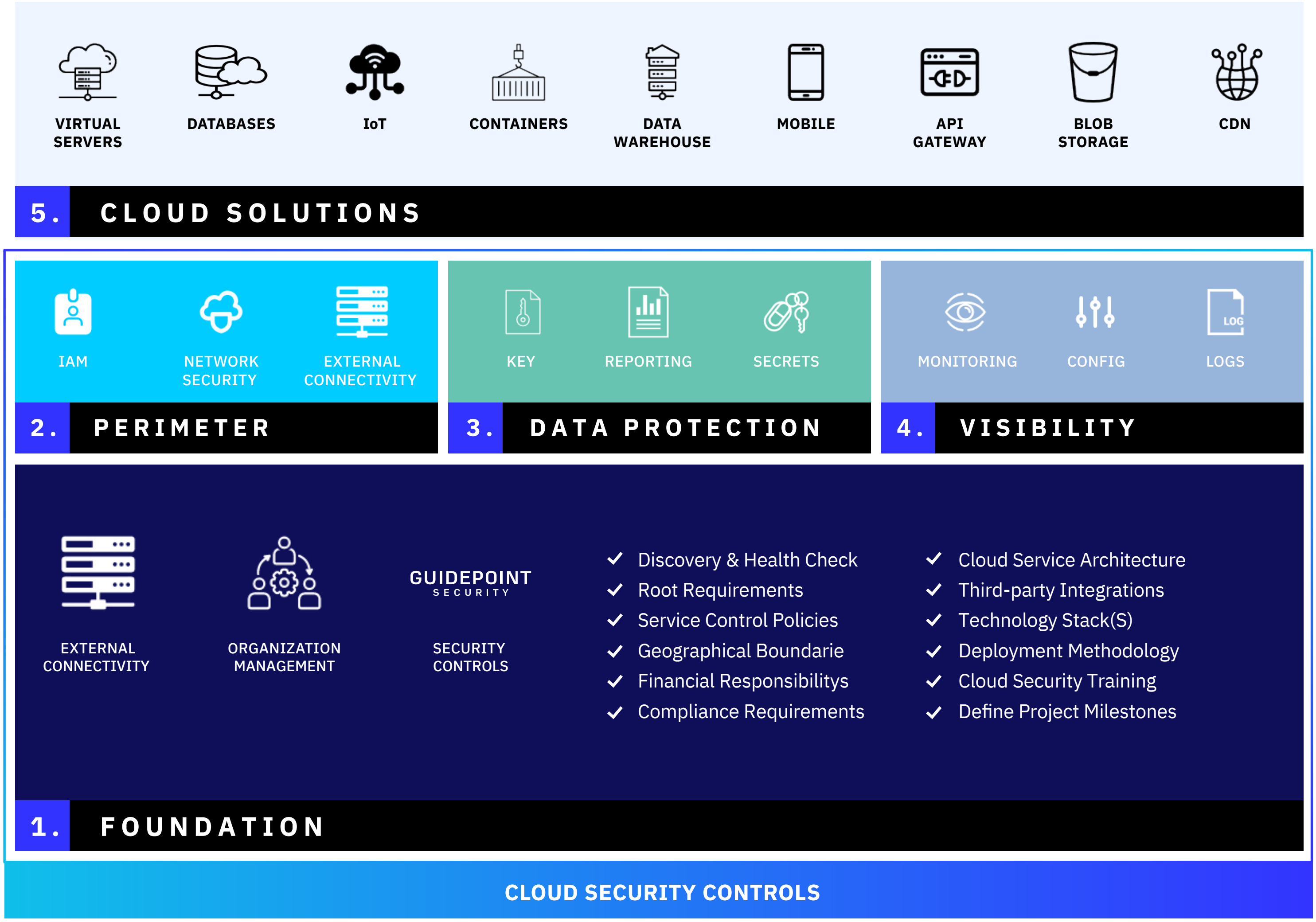
There are many steps for setting your cloud security course. However, as with building construction it's imperative to understand building regulations (governance) and ensure that you stay within those boundaries (project management) or you'll find yourself correcting expensive assumptions. Start by creating two teams: Governance and Project Management. You can build on these teams and educate them on your strategy. You can also hold foundational and strategy meetings to set the direction and identify your targets and goals so they don't have to be addressed later on in the process.

- ✓ **Governance Team –** Used to define the standards, compliance mandates, and the direction an organization will take.
- ✓ **Project Management Team –** Sets the pace and ensures the project remains on course. This team is vital when you stop to consider how quickly activities will move in the environment.

You should examine how the changes apply to your AWS environment, as well as how it applies to SaaS applications. There are different outcomes and requirements for each environment, and you must decide what situation will be most advantageous to meeting your organizational goals, needs, objectives, and security requirements.

Successfully Implement Cloud Security: The Five Phases

When it comes to successfully constructing and implementing cloud security, the first four phases are where you define your security controls and strategy, while the fifth phase is implementing the cloud solution(s), i.e. the business layer.



VIRTUAL SERVERS · DATABASES · IoT · CONTAINERS · DATA WAREHOUSE · MOBILE · API GATEWAY · BLOB STORAGE · CDN

5. CLOUD SOLUTIONS

IAM · NETWORK SECURITY · EXTERNAL CONNECTIVITY

2. PERIMETER

KEY · REPORTING · SECRETS

3. DATA PROTECTION

MONITORING · CONFIG · LOGS

4. VISIBILITY

EXTERNAL CONNECTIVITY · ORGANIZATION MANAGEMENT · GUIDEPOINT SECURITY SECURITY CONTROLS

- ✓ Discovery & Health Check
- ✓ Root Requirements
- ✓ Service Control Policies
- ✓ Geographical Boundarie
- ✓ Financial Responsibilitys
- ✓ Compliance Requirements

- ✓ Cloud Service Architecture
- ✓ Third-party Integrations
- ✓ Technology Stack(S)
- ✓ Deployment Methodology
- ✓ Cloud Security Training
- ✓ Define Project Milestones

1. FOUNDATION

CLOUD SECURITY CONTROLS

PHASE ONE

The Foundation

The most important aspect to the five phases is making sure to build a strong, firm foundation. You must initially determine your current posture and then decide what your baseline is and identify any major gaps that need to be remediated sooner rather than later. As part of this process, you'll want to be able to answer questions such as:

- Have you identified a current posture and baseline?
- (AWS) How will root accounts be managed?
- How will you address exposure and threats from new cloud services before they are adopted or deployed?
- Which compliance requirements impact your business and will drive your architecture (governance)?
- A "we run everything" tech stack is fine, but how does that impact standardization, security, efficiency, and agility?
- Are you ok with managing multiple authentication mechanisms separately?
- Is your team adequately trained to adopt cloud computing?

Other areas which you should consider include:

- What are the roles and responsibilities going to be?
- What services are you going to use?
- Are you going to use cloud-native encryption?
- Should you start talking to a vendor to bring in third-party solutions?
- Are you going to be multi-cloud?
- Is your team adequately trained to adopt cloud computing? Are your project managers ready for not just Agile project management, but also ready to support an integrated team (DevOps/ DevSecOps)?

PHASE TWO

The Perimeter

Phase Two focuses on the new boundary—that is, determining what your perimeter strategy is going to be. You can have a false sense of security, believing your network security is really strong, while authorization and authentication are weak. Any compromise of a privileged cloud account will supersede anything you're doing on the network. We recommend that as you are building out your program, one of the early items you address is including identity access management for the cloud along with a strong authorization process. This is really going to dictate the true security posture of your cloud environment.

A lot of good patterns for network security and network topologies in the cloud have emerged. For example, Transit Gateway in AWS or hub-and-spoke Virtual Private Clouds are almost always found when we conduct security assessments. Once you have addressed the perimeter, you should have identified roles, a secure network architecture, and more importantly, a model to ensure that least privilege policies are maintained within your environment(s).

PHASE THREE

Data Protection

Encryption, key management, and secrets management services will also be a major factor when discussing data protection. You are going to have to decide whether you want to leverage a third-party solution for critical services such as certificate management, data encryption, and secrets management. Or, do you want to leverage the cloud-native service?

Here's a spoiler alert—native key management services in the cloud **CAN** be trusted.

With proper implementation and oversight they are secure. Native cloud encryption could be operationally efficient and cost efficient, but again, you will want to make sure you have got the right strategy behind the decision.

PHASE FOUR

Visibility

Visibility is very important but also sometimes presents the most challenges. When done right, you should be able to build a story around activity in a cloud environment. In order to efficiently collect, organize, and gain the right performance with your data, you need a logging platform that enables you to ingest logs and easily build search queries, or simply have an efficient way to identify particular events or anomalies.

Being able to adjust the amount of data that is coming in will give you the right platform to build your dashboards in order to gain critical visibility. You will need to log your cloud API activity and your network traffic as well as infrastructure changes.

If you are still leveraging infrastructure as a service (IaaS), you will still need to log your OS logs (e.g. (/var/log/secure, /var/log/message, windows logs, etc.). This is why it is so important to have the right logging platform from the beginning. Other services will also manage inventory, including tracking and discovering new inventory.

During the Visibility phase you will want to make sure to search for the unknown events and threats. You will need a platform that can support the following capabilities and perform the following activities:

- A logging platform that helps you understand cloud events in addition to other events so you can correlate activity.
- Log cloud API activity, network traffic, infrastructure changes.
- Automate your Change Advisory Board—all cloud resources and changes to them are logged and can be prevented or rolled back.
- Don't waste time going down unnecessary rabbit holes; instead focus on the important things to look for, including: excessive denied API requests, anomalies in cloud API usage (even with successful least privilege policies), and change in baselines such as increased compute capacity or network ingress/egress traffic.

PHASE FIVE

Cloud Solutions

At this point, with a firm foundation and the other four phases implemented, you can address your cloud solutions. Regarding this phase, here are some considerations:

- Are compute instances following configuration management and golden Amazon Machine Image (AMI) processes? Are they hardened? Are roles/ service principals used only when needed?
- Do you have the necessary visibility and continuous monitoring to ensure improvements to access controls?
- Have you deployed acceptable web application protection based on your platform as a service (PaaS) architecture?
- Are you prepared to accept the adoption of new cloud services and are you in a good place to tackle common denominators related to public cloud service providers?
- Can you align to industry frameworks to meet your compliance requirements?

Putting it All Together

We've learned, through successful implementations, that this five-phase methodology facilitates a consecutive thought process. By first identifying foundational elements such as compliance mandates, top-level cloud account management, technology stack standards, network topology, and more... the questions that are asked and the decisions that need to be made later will become easier.

For instance, if we work backwards from Phase 5, using compute instances / virtual machines as an example:

- What do need we need to log within and around the compute instance, virtual machine, container, or Lambda function? This was decided in Phase 4.
- Where do we send our logs and what events are we looking for (e.g., using VPC Flow logs)? Let's say we made the decision to log these services to CloudWatch Logs or to an S3 Bucket. Decided in Phase 4.
- Do we encrypt the cloud native logging stores, e.g. CloudWatch Logs or S3 or the Azure Storage Account? This was decided in Phase 3.
- Who or what has access to not only the storage locations but also the encryption keys in KMS?This was decided in Phase 2.
- Why are we encrypting these logs? This was part of the governance decisions made in Phase 1 driven by a compliance requirement.

When Phases 1 through 4 are grouped together, they'll form the basis for our cloud security controls framework. Will we have a solution for every use case? Realistically no, especially given the evolving nature of the cloud. However, this methodology gives us a sequential pattern to follow instead of trying to tactically solve individual, smaller problems.

How GuidePoint Security Can Help You Innovate and Deliver on Your Cloud Security Strategy with AWS Marketplace.

When it comes to cybersecurity and the cloud, there is no one-size-fits-all approach. GuidePoint Security can help you tackle all the challenges associated with your organization's AWS cloud security through a wide range of services that include:

Cloud Readiness Assessment

The Cloud Readiness Assessment provides a holistic analysis of your operational environment to include the people, processes, and technologies relevant to the cloud. GuidePoint architects work with our customers to develop a cloud readiness roadmap guiding clients in a secure migration to the cloud. The roadmap builds on industry frameworks such as the Cloud Security Alliance Cloud Controls Matrix and NIST 800-145 as well as published reference architectures from cloud service providers.

Cloud Security Health Check

The Cloud Security Health Check provides a detailed architectural review of your Amazon Web Services environment. Our architects and engineers work with you to understand the operational needs of your cloud environments and assess your current security posture to provide relevant, prioritized, and actionable remediation efforts.

Cloud Security Visibility Assessment

Organizations are often surprised to discover how many sanctioned and unsanctioned cloud applications are in use across their environment. Furthermore, they usually lack the technology to control the usage of those cloud services or the data stored therein. The Cloud Security Visibility Assessment provides you with a detailed look into the actual cloud usage within your enterprise as well as mitigation strategies to secure data within sanctioned services and control data in unsanctioned services.

Cloud Security Architecture and Strategy

Our architects and engineers have years of operational experience in cloud, security, and enterprise IT. We are able to offer a diverse array of cloud engineering services, to include special projects, vulnerability management, systems hardening, cloud security governance, DevOps integration, systems design, and more.

GuidePoint Security is an authorized AWS Marketplace Consulting partner.

Conclusion

To achieve cloud security, we recommend going through the five-phase methodology that we've outlined. To summarize, we'll review some very important takeaways about the five phases of Cloud Security Architecture, phase by phase.

For phase 1: Foundational Setup, make sure you establish a cloud steering committee for oversight and identify any compliance requirements you need to consider. You should also define your cloud baseline and monitor it, identify your AWS account owners, provide your staff with cloud adoption and cloud security training, and define your spend thresholds and alerts.

In phase two, make sure you define and implement a responsibility assignment matrix (RACI) model based on current roles and your future cloud roadmap, update permissions based on actual activity in the cloud, ensure egress visibility is in place for awareness of what is leaving your cloud, and always monitor and alert on deviations from your baseline.

When it comes to the data protection phase, follow through and act on encryption requirements, and work with your developers to incorporate secrets management using native cloud services. Don't shy away from cloud-native data protection services. And as in the previous phase, monitor and alert on deviations from your baseline.

In phase four, to ensure proper visibility, you must implement known patterns of CloudTrail, VPC Flow Logs, Config, Guard Duty, Activity Logs, Security Center and consolidate your logs somewhere. Identify what to alert on, who should respond, and how to remediate cloud security event. And as in previous phases, monitor and alert on deviations from your baseline–in this case anomalies, failed API calls, etc.

Finally, when looking at cloud solutions, build and implement infrastructure as code (IaC) templates to standardize deployment of cloud resources. Use a "golden image" process and alert on non-approved images that are being used or deny them from being deployed. Make sure any new cloud solutions have been approved by or are visible to the cloud steering committee.

Remember, cloud environments are diverse and while some security leaders have the foundation, some just need a blueprint. There are historical challenges and new challenges to be aware of. When looking forward, is multi-cloud something to consider? Establishing project management patterns for cloud computing will help ensure you have a manageable process that ties in security with your business operations.

With this five-phase methodology implemented, you're now ready to enjoy the benefits of the cloud, while ensuring it is secured.

WORK WITH US

GuidePoint Security helps you navigate the challenges of securing an AWS-cloud environment. We provide deep cybersecurity expertise with a team of AWS-certified practitioners and a wide range of cybersecurity offerings such as solution implementation, assessments and technology support services.

Find GuidePoint Security in the AWS Marketplace.

aws marketplace

ABOUT THE AUTHOR

Jonathan Villa

Jonathan Villa is the practice director for cloud security at GuidePoint Security. Jonathan has spent more than 21 years across different disciplines including application development and security, web development, compliance, middleware administration, and network security. Since the mid-to-late 2000s, Jonathan has built and deployed his own solutions to AWS out of necessity. He now shares that experience with customers.

GUIDEPOINT
SECURITY

2201 Cooperative Way, Suite 225, Herndon, VA 20171
guidepointsecurity.com • info@guidepointsecurity.com • (877) 889-0132