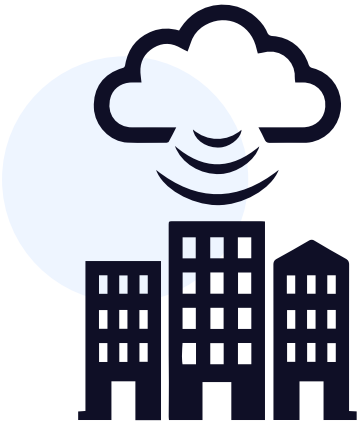
WHITE PAPER

The Five Phases of Cloud Security Architecture

GUIDEPOINT®
SECURITY

This paper examines key points you need to consider when defining your cloud security strategy and delves into five phases of cloud security architecture.

Identifying an effective cloud security architecture depends on how your organization defines the cloud, as well as the operational model chosen to build and manage your environment. (Operational models include IaaS, PaaS, SaaS, and hybrid.)



In construction, a building must begin with a strong foundation.

This foundation helps ensure that the building can withstand numerous threats from sweltering temperatures, violent hurricanes, or freezing blizzards. All the necessary steps and procedures to build a foundation must be followed. If shortcuts are taken, the foundation may become unstable, leaving the entire structure vulnerable to risks and potentially catastrophic damage.

Depending on your unique needs, the edifice you build, the steps to construct it, and its functionality will all vary. In other words, architects and developers – in buildings and in cloud security – need to right-size their approach. As with a residential or commercial structure, successful Cloud Security Architecture begins with a best-fit, well-planned, "built-to-code," solid foundation.

Cloud isn't simply "cloud." Each major Cloud Service Provider (CSP) is different. 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.

Organizations have adopted various strategies to deploy public cloud services, ranging from computing and data analysis to storage and serverless applications. This discussion centers on the five phases of cloud security architecture, providing a comprehensive framework to address the unique challenges of securing cloud environments.

Integrating security from the outset is essential—it's not something to add-on or address later. Depending on your strategy and time-to-market goals, you'll face a crucial choice between relying solely on native cloud security controls or incorporating third-party platforms for enhanced protection. Each option affects scalability and adaptability. At the same time, it's critical that you design a "future-proof" security framework. With the speed of innovations - such as the widespread adoption of AI-driven tools - your security must remain flexible to adapt to evolving technologies and risks.

Drawing on successful cloud implementations, we've developed a practical and repeatable methodology for establishing robust cloud security. It effectively tackles today's challenges while enabling your organization to seamlessly adapt to future advancements, protecting your operations, and fostering long-term growth.

Cloud Logging, Encryption, Authorization

When it comes to cloud logging, encryption, and authorization, here are issues to consider:

Cloud logging:

- What do we log?
- Where do we centralize our logs?
- Do we encrypt the logs?
- How do we interpret our logs?

Encryption:

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

Authorization:

- How do we achieve and manage least privilege within a complicated entitlement ecosystem?
- Where do we have non-human identities (NHI)? (Authorization question)

You also may need to address poor management solution authorization and NHI, one of the more challenging issues.

Where to Start ?

Occasionally, security leaders express concerns about cloud security because they are unfamiliar or have limited knowledge of the various and respective Cloud Service Provider capabilities. Sometimes, it's important to pause and host more discussions 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 developed and what makes the most sense.

Once you've decided on an approach to adopt or further migrate to the cloud, it's essential to assess security considerations before implementation begins. If you have already deployed cloud resources, it's important to maximize your visibility and gain a clearer understanding of your security posture. This can involve utilizing a combination of cloud native tools 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). Otherwise, you may find yourself correcting expensive assumptions. Start by creating two teams: Governance and Project Management. You can extend 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 in the process.

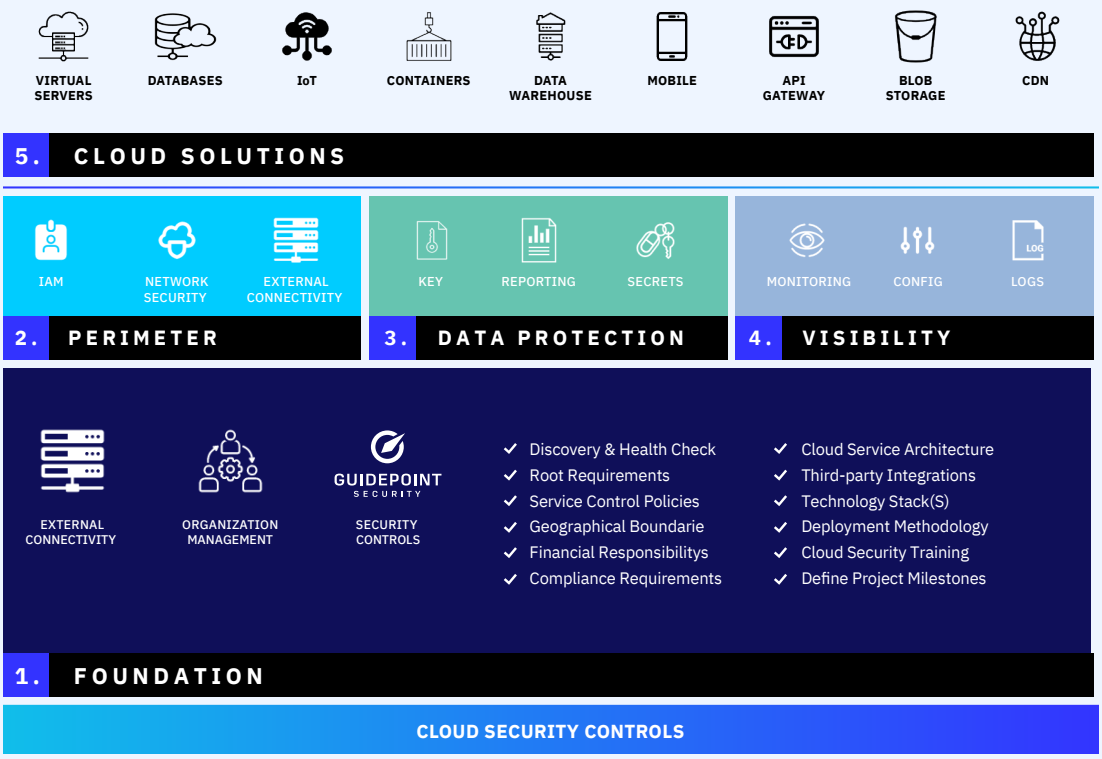
- Project Management Team – Sets the pace and ensures the project remains on course. This team is vital when you stop to consider how quickly activities will move in the environment.

You should examine how the changes apply to your AWS or Azure environments 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.

- Cloud Governance Team – Used to define the standards, compliance mandates, and the direction an organization will take.

Successfully Implement Cloud Security: The Five Phases

Reading from the bottom-up, use this chart to navigate the 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.



PHASE ONE

The Foundation

The most important aspect of the five phases is to build a strong foundation. You must initially determine your current posture. Then decide what your baseline is, and finally, 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? (This may include a recent adoption or pivot to AI.)
- Which compliance requirements impact your business and will drive your architecture (Cloud 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 that you should consider including:

- Have you defined roles and responsibilities? Did you develop a RACI?
- Which cloud services (IaaS, PaaS, SaaS) 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 (perhaps for a multi-cloud environment)?
- 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 – determining what your perimeter strategy is going to be. You can have a false sense of security, believing your network security is 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 build out your program, one of the early items you address is identity access management (IAM) for the cloud, along with a strong authorization process. This will 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 gateways with hub-and-spoke virtual networks are almost always found when we conduct security assessments. Visibility and control over both North and South traffic, as well as East and West, will help reduce the blast radius in a compromise. Once you address perimeter security, you should have clearly 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 the right strategy behind the decision.

In multi-cloud environments, third-party platforms can provide a unified layer of visibility, governance, and security across those CSPs. Adopting a cohesive solution and uniting visibility and control across multiple cloud providers can streamline management, reduce risk, and enhance agility to ensure your cloud strategy remains scalable and resilient.

PHASE FOUR

Visibility

Visibility is very important, but it can sometimes present the most challenges. When done right, you should be able to build a story around activity in a cloud environment. 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 a particular event or anomalies.

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

If leveraging Infrastructure as a Service, you still need to log 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 outset. Other services will also manage inventory, including tracking and discovering new inventory.

During the Visibility phase, make sure to search for any unknown events and threats. **The platform you select should support the following capabilities and perform the following activities:**

- A logging platform that helps you understand cloud events and other events to correlate activity.
- Log cloud API activity, network traffic, and infrastructure changes.
- Automate the 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; understand the important things to look for, including excessive denied API requests, anomalies in cloud API usage (even with successful least privilege policies), and changes in baselines such as increased compute capacity or network ingress/egress traffic.

PHASE FIVE

Cloud Solutions

When you reach this point, with a strong foundation and the prior four phases implemented, you should address the cloud services that align with your organization's business objectives. These solutions often underpin essential applications or drive operational needs, directly contributing to organizational success and productivity.

Organizations frequently encounter recurring questions about network security, entitlements, encryption, and compliance while adopting new cloud services. **This methodology is designed to preempt such challenges by establishing a strong base architecture, ensuring these common issues are resolved proactively and efficiently.**

- When using Functions as a Service, a service that relies on entitlements, the Perimeter phase should have identified the standard operating procedures for managing entitlements.
- When working with non-human identities, the Foundation phase should have identified third-party integrations that the environment or application will need.
- With the adoption of AI, the data protection phase should have established standards for data segmentation, so that an organization can quickly identify where sensitive data is stored.
- With ever-growing threats to data, the Visibility phase should have identified a pattern to identify indicators of attack and compromise on the environment, or identified a third-party solution that specializes in cloud detection and response.
- Ensuring continuous compliance is a challenge. However, the Foundation phase should have identified the required policies, the standards to provide guidance, and code to enforce it all.

Putting it All Together

We've learned, through successful implementations, that this 5-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. This methodology is applicable across diverse cloud security architectures, including SaaS, IaaS, PaaS and hybrid or multi-cloud environments. **Organizations also need to adapt security controls based on the service model in use—for instance:**

- SaaS environments require more robust access management, data protection, and compliance controls to ensure third-party services align with security policy.
- IaaS deployments will need to secure virtual machines, storage, and network configurations within public cloud providers.

For instance, if we work backward from Phase 5 (Cloud Solutions), using compute instances / virtual machines as an example:

- What do we need to log within and around the compute instance, virtual machine, container, or Lambda function? This was decided in Phase 4 (Visibility).
- Where do we send our logs, and what events are we looking for? For example, using AWS VPC Flow Logs or Azure NSG Flow Logs. You may decide, for instance, to log these services to CloudWatch Logs or to an S3 Bucket or in Azure a Storage Account. Also, decided in Phase 4 (Visibility).
- 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 (Data Protection).
- Who or what has access to not only the storage locations but also the encryption keys in KMS and Key Vault? This was decided in Phase 2 (Perimeter).
- Why are we encrypting these logs? This was part of the governance decisions made in Phase 1 (Foundation), driven by a compliance requirement.

When Phases 1 through 4 are grouped together, they'll form the basis for our cloud security controls framework. An organization moving to a multi-cloud model, for instance, could use this methodology to align security policies across AWS and Azure, ensuring consistent logging, access control, and compliance enforcement. By structuring their approach around the five phases, they can reduce security gaps and streamline their cloud security architecture.

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.

GuidePoint Security Can Help with Your Cloud Security Architecture

The conversation is no longer “whether you are moving to the cloud” but rather “how many cloud services are you using?” (Don’t forget about shadow IT!) We can help you tackle all the challenges that lead to cloud security for your organization through a wide range of services that include:

Cloud Readiness Assessment

The Cloud Readiness Assessment delivers a comprehensive evaluation of your operational landscape, encompassing the people, processes, and technologies critical to cloud adoption. GuidePoint architects collaborate closely with clients to craft a tailored cloud readiness roadmap, ensuring a secure and efficient migration to the cloud. This roadmap leverages industry standards like the Cloud Security Alliance Cloud Controls Matrix and NIST 800-145, along with established reference architectures from leading Cloud Service Providers.

Cloud Security Visibility Assessment

Organizations are often surprised to discover how many sanctioned and unsanctioned cloud applications are in use across their environment. Compounding this, 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 Health Check

The Cloud Security Health Check offers a thorough architectural analysis of your Amazon Web Services or Microsoft Azure environments. Our team of architects and engineers partners with you to understand the specific operational demands of your cloud infrastructure. We evaluate your existing security posture to deliver clear, prioritized, and actionable recommendations for improvement.

Cloud Security Architecture and Strategy

GuidePoint architects and engineers bring extensive hands-on experience across cloud environments, cybersecurity, and enterprise IT. We provide a wide range of cloud engineering services, including special projects, vulnerability management, system hardening, cloud security governance, DevOps integration, system design, and more.

GuidePoint partners with Cloud Service Providers (CSP) including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.

Conclusion

To achieve cloud security, we recommend going through this Five-phase Methodology. In review, here are the most important takeaways:

PHASE ONE, THE FOUNDATION: Establish a Cloud Steering Committee for oversight and identify any compliance requirements you need to consider. Define and monitor your cloud baseline, identify key account owners, provide staff with cloud adoption and cloud security training, and define spend thresholds and alerts.

PHASE TWO, THE PERIMETER: Define and implement a model based on current roles and your future cloud roadmap, update permissions based on actual activity in the cloud, solve the NHI problem, and ensure egress visibility is in place for awareness of what is leaving your cloud. And, constantly monitor and alert on deviations from the baseline.

PHASE THREE, DATA PROTECTION: Follow through and act on encryption requirements, and work with your developers to incorporate secrets management. As with the previous phase, monitor and alert on any deviations from your baseline.

PHASE FOUR, VISIBILITY: Make sure to implement known patterns of CloudTrail, VPC Flow Logs, Config, Guard Duty, and Activity Logs, and consolidate your logs somewhere. Identify what to alert on, who should respond, and how to remediate cloud security events. As with previous phases, monitor and alert on deviations from the baseline – in this case, anomalies, failed API calls, etc.

PHASE FIVE, CLOUD SOLUTIONS: Finally, when evaluating cloud solutions, build and implement IaC templates to standardize the 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. While some security leaders have the foundation, others 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 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.

ABOUT THE AUTHOR

Jonathan Villa

Jonathan Villa is the practice director for cloud security at GuidePoint Security. Jonathan has spent more than 24 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

WP-CSA-102020-01