The Positive Way

WAVESTONE

Strategy Brief

Ensuring Cloud Security Throughout Your Cloud Solution Lifecycle

Efficiently Scaling, Optimizing, and Automating Your Cloud Solutions with Proactive Cybersecurity

By: Keith R. Worfolk

INTRODUCTION – BUILDING CLOUD SECURITY PROACTIVELY AND DYNAMICALLY IS THE NAME OF THE GAME IN THE CLOUD!

Cybersecurity is the enabling lifeblood for any growing or transforming IT footprint of an organization, whether in or outside of Cloud. Without it at the forefront, such growing, scaling, and changing of (Cloud, etc.) solutions can only increase your organizational risk and threat surface. With it intrinsically integrated into your overall Cloud strategy and solutions via mature operational processes and tools, you will enable worry-free (or at least well-managed) expansion of your Cloud solutions and capabilities – with comprehensive maturity, including built-in security that scales and adapts to your changing Cloud footprint.

Note that, at its core, the issues of cybersecurity in the Cloud do not change dramatically from those of data centers and other on-prem IT footprints (i.e., identity management, network perimeter and behaviors, data protection, configuration management, and systems access, to name some key ones). However, the Cloud does significantly change many aspects of solution design, implementation, and operations, including security needs.

Cloud environments are virtual ones, so all infrastructure components – servers, compute power, storage, network components (routers, firewalls, intrusion detection and prevention), gateways, antivirus, and malware protection, etc. – are presented and operated as virtual services within a Cloud Service Provider (CSP) platform and its environments.

Hence, this type of Cloud architecture simplifies things in many ways: hardware doesn't need to be installed, storage is provided, and compute capabilities can be efficiently scaled up or down depending on current needs (not tied to pre-built data center capacities). Deploying workloads in the Cloud often involves complex sets of microservices and serverless instances that are configured to function within flexible architectures that can (and do) change substantially every few minutes (or even seconds!).

This creates a constantly changing security footprint and threat surface that must be proactively and dynamically addressed, especially as most organizations are seeing their most valuable information assets shift from on-prem resources to Cloud environments. These very fluid Cloud architectures lead to the fact that traditional data center defenses, built to protect a defined perimeter by monitoring and controlling data that moves in and out of a well-defined network environment, will not be as (or sufficiently) effective in Cloud solution environments.

Cybersecurity implementations in the Cloud are indeed different from on-prem because the technological paradigms are so unlike traditional on-prem solutions (e.g., now based more on APIs, microservices, and dynamic configurations). As we'll see, Cloud Security implementations also vary with the choices an organization makes regarding its Cloud solution model – architectures, designs, and configurations (i.e., infrastructure resources vs. CSP or 3rd Party services).

What also changes in regard to cybersecurity within the Cloud is an organization's RACI; and depending on your predominant Cloud solutions model – IaaS, PaaS, and/or SaaS – you will have relatively different activities and skills needs to build, secure, and maintain your Cloud environments. Hence, adaptive cybersecurity that addresses the many ways cloud solutions can (and will) be implemented is a key to your Cloud cyber success and will make the difference between a good or bad Cloud Security strategy.

So how do you get there – to efficiently grow and scale your Cloud Security capabilities while staying a step ahead of your very dynamic cloud footprint (and evolving vulnerabilities)? Firstly, with a Cloud Security-first strategy: this is needed to ensure your security maturity is proactively integrated into your overall Cloud capabilities maturity and roadmap. We'll explain more of what this entails in this security brief.

Cloud Security – Guiding Principle #1:

Build a Cloud Security-first strategy and approach to lead with security capabilities as an enabler (as you lay the Cloud journey road) for overall (secure) Cloud solutions growth and maturity.

Hence, Cloud Security should be “Job 1” to enable the solutions and capabilities of your organization’s Cloud strategy. It should consistently be ahead of the solutions you are looking to migrate to and/or build into your Cloud footprint. It must also be the type of security architecture/design that proactively addresses your organization’s unique Cloud solutions and security needs, current and planned.

Complementing “Job 1” to design-in and build-in security proactively as an enabler to your Cloud solutions and expanding footprint, you must also address the dynamic nature of Cloud architectures. This means your Cloud Security footprint, processes, and tools must be designed to stay ahead (very different from on-prem security architectures) of the multi-layered and changing security needs of many solution types. These are regularly built as combinations of infrastructure, configurable services, code, APIs, and elastically scaling resources that can be complex for security risk management, and clearly cannot be static in its security coverage.

The best way to do this is via a multi-layered security strategy, including defenses that:

Block unauthorized access to the network (of course, the outermost layer); and

Prevent unauthorized activities inside the network (one to several other layers, depending on what we are protecting)

For an attacker to be successful, they must bypass all defense layers. Note the second part of layered defenses generally takes on dynamic aspects such as context-driven monitoring of behaviors within the network, based on specific workloads (solutions, applications, data, etc.) involved, and can also include timing components as to whether certain actions are expected or allowable for an access or workload.

For example, as many as 85% of new data breaches now have a human element. The failure of staff (accidentally or purposely) to follow best practices give adversaries too many opportunities to intrude, infiltrate, and attack your Cloud footprint. Only a defense-in-depth strategy, with unified coverage across hybrid (Cloud and on-prem) and multi-cloud environments, can close such gaps.

Further, as we'll see, these dynamic and potentially highly complex multiple layers of controls needed are most effective when managed via a centralized security management platform. For this capability, you may have to go outside of your CSP's standard security tools and dashboards. From such a centralized security platform, you will:

Continually monitor and detect risks introduced by new and updated cloud assets, servers, and containers

Alert solution and resource owners (in real-time) of detected threats (as configured or via AI-driven behavioral analysis)

Potentially inform solution owners and administrators of how to fix the discovered issue

Progressively automate remediation of common issues and quarantine suspicious workloads automatically, which can shrink the attack surface in real-time

Hopefully, it's becoming quite clear that traditional (on-prem) security processes, tools, and operations are not well-equipped for these dynamic Cloud Security complexities. Thus, it becomes a strategic security imperative to plan for layered defenses in the Cloud as well as new types of security processes and tools to underpin the necessary dynamic monitoring, alerts, etc. of your Cloud environments. As we look at ways to build out your Cloud Security strategy, capabilities, and maturity in this strategy brief, we'll revisit this concept more than once.

Cloud Security – Guiding Principle #2:

Build a layered Cloud Security strategy and defenses to dynamically address your unique growing and changing Cloud solutions and footprint, including:

a) Go beyond traditional controls to configure monitoring and anomaly alerts for your specific workloads, resources, and (policy-driven) behaviors

b) Consider complementary 3rd Party Cloud Security tools to consolidate and strengthen your multi-layered security capabilities

CLOUD SOLUTION LIFECYCLE REVISITED – INCLUDING SECURITY IMPLICATIONS IN EACH PHASE

To address these first two (Job 1 & 2) strategic Guiding Principles for Cloud Security, and others forthcoming, let's start with a refresher of the Cloud Solution Lifecycle (CSL). This is where your desired Cloud Security posture needs to manifest itself to be efficient and pervasive throughout your Cloud solutions comprising your expanding and dynamic footprint. This is true whether a Cloud solution is the product of on-prem migrations to the Cloud, or a product of new Cloud-native development. As you'll see, the entanglements of Cloud Security requirements and ways to address these are similar in either case.

Considering a typical Cloud Solution Lifecycle (see Diagram 1 below), we can see that all Cloud solutions do indeed traverse these Lifecycle Phases, at least once upon creation in the Cloud (whether migrated or developed), and potentially multiple times in the case of ongoing solution releases.

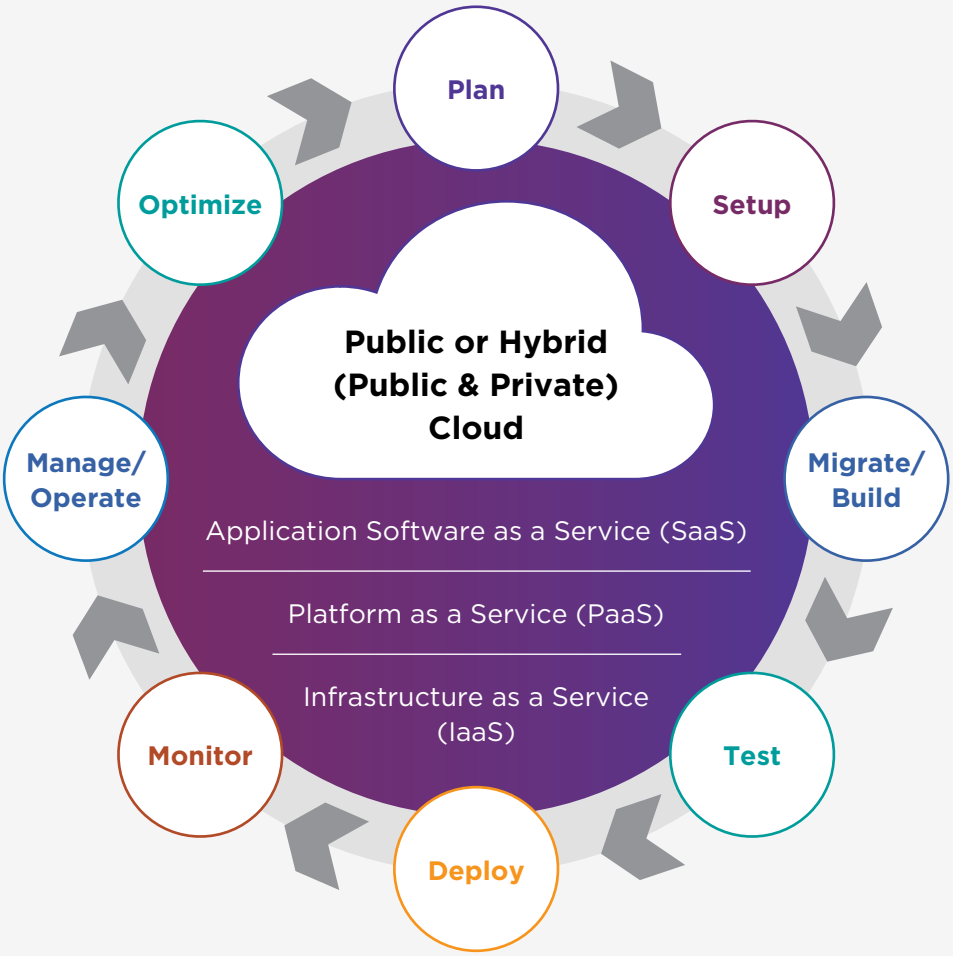


Diagram 1: Cloud Solution Lifecycle (CSL) – All Cloud Solutions go through these Phases

There are three basic observations we can make regarding the Cloud Solution Lifecycle (CSL), and how an organization should manage it, that dramatically affects your team's Cloud solution creation, operational, and management capabilities as well as its (preferably proactive) security incorporation.

General Observations about the Lifecycle – Creating a Cloud solution's target state:

1. Proactively design and develop a solution's optimal future state (security, performance, cost, etc.) in the Cloud, whether migrated to or newly built, by defining and preparing for this as early as possible (practical) – in the Plan, Setup, and Migrate/Build Phases

2. If (security, efficiency, etc.) transformations or optimizations are not addressed in the early Phases, such advancements can only be achieved much later (reactively) by retrofitting improved solution designs during post-Deployment Phases. In this case, there are a couple of strategic problems your teams will have to consider (in a later Plan Phase, release, etc.):

   a. Your security improvement options may become limited by the way you initially designed and stood up the Cloud solution; and

   b. Both IT and Business stakeholders will have lived with built-in deficiencies (i.e., security risks and/or inefficiencies) until the time when these are corrected (perhaps months later in a follow-on release!)

3. While the CSL may resemble an SDLC at first glance, you'll notice important differences, such as the optional Migrate and Optimize Phases, and additional "as-a-Service" design options (from which your teams can choose). Also note that the CSL should generally be utilized as part of an agile SDLC methodology for best execution; it's not itself an SDLC

Thus, don't plan for (or accidentally adopt) a strategy for suboptimal solution target architecture or designs (e.g., mass Lift n' Shift, predominantly IaaS) for your migrations, or employ non-Cloud-native development practices for new solution implementations. Not only are these short-sighted, tactical approaches that may seem a faster way to get into the Cloud, but they will leave you with a large backlog of needed improvements (including security, performance, etc.) and built-in risks that could have been better addressed upfront in initial planning and design activities.

At a minimum, use your Plan and Setup Phases to proactively plan and design for your desired level of security optimization of solution deployments; and understand how any security implementation deferments will affect your security profile, management, costs, and efforts to correct later.

Cloud Security – Guiding Principle #3:

Build Security proactively into your Cloud solutions early in planning and design activities. Even if you choose to defer certain security optimizations upon initially standing up your Cloud solution, understand what you are foregoing in terms of risks, costs, and later effort to correct.

Looking a little deeper into the specific security implications throughout the Lifecycle, we can derive the following three important considerations that should be addressed by your security teams during key CSL Phases.

Security Considerations during the Lifecycle – Creating a Cloud solution's security target state:

1. Within a comprehensive Cloud Strategy program and operating model, all solution security implementations and operational processes should address the overall changing Cloud footprint and threat surface realized during each Phase. The security impacts of a particular solution's design and implementation for target security state is not as important as the overall changing Cloud Security posture; understand and balance both the local (solution) and enterprise-level impacts

2. The target security design and implementation accommodations (architecture, controls, configurations, etc.) established during earlier Phase activities (i.e., Plan, Setup, and Migrate/Build) generally provide better (proactive, design-integrated) security than those identified and enacted upon later in post-Deployment Phases (e.g., discovered during Test, Monitor, Manage/Operate, or Optimize activities), or that are deferred to later Lifecycle iterations/releases. See "General Observations about the Lifecycle" above for problems created by deferring security concerns until later Phases or cycles

3. While the CSL can seem to imply waterfall activities for security design/implementation, the Cloud Security target definitions, designs, and implementation actions are intended to be addressed within an agile DevSecOps approach for best execution

The bottom line regarding Cloud Solution Lifecycle usage for secure implementations is that shifting security design and implementation considerations "upstream" to earliest possible Phases will give you stronger and earlier security benefits. Note that this flies in the face of organizations that have been (or are considering) adopting mass "Lift n' Shift" (IaaS migration) efforts and deferring modern Cloud design accommodations, including security, to sometime after moving basic workloads as they were previously designed (for on-prem VMs). For security reasons and a few others, such strategies are often rethought later as (upon further review) being too inefficient and insecure… which is ironic considering this was once thought to be the fastest way to initially build your Cloud journey ("get to the Cloud fast!").

Cloud Security – Guiding Principle #4:

Cloud Security should continually be refined and enacted throughout the solution Lifecycle; and related to this, security will be most mature in organizations that: a) Shift solution security actions to earlier Phases; and b) Employ an agile DevSecOps approach to all solutions

CLOUD MATURITY MODEL REVISITED – INTRODUCING THE CLOUD SECURITY MATURITY MODEL (CSMM)

You are likely familiar with Cloud capabilities roadmaps and maturity models if you've begun your Cloud journey. A strategic Cloud capabilities Maturity Model that can be used to grow your Cloud capabilities is shown below in Diagram 2.

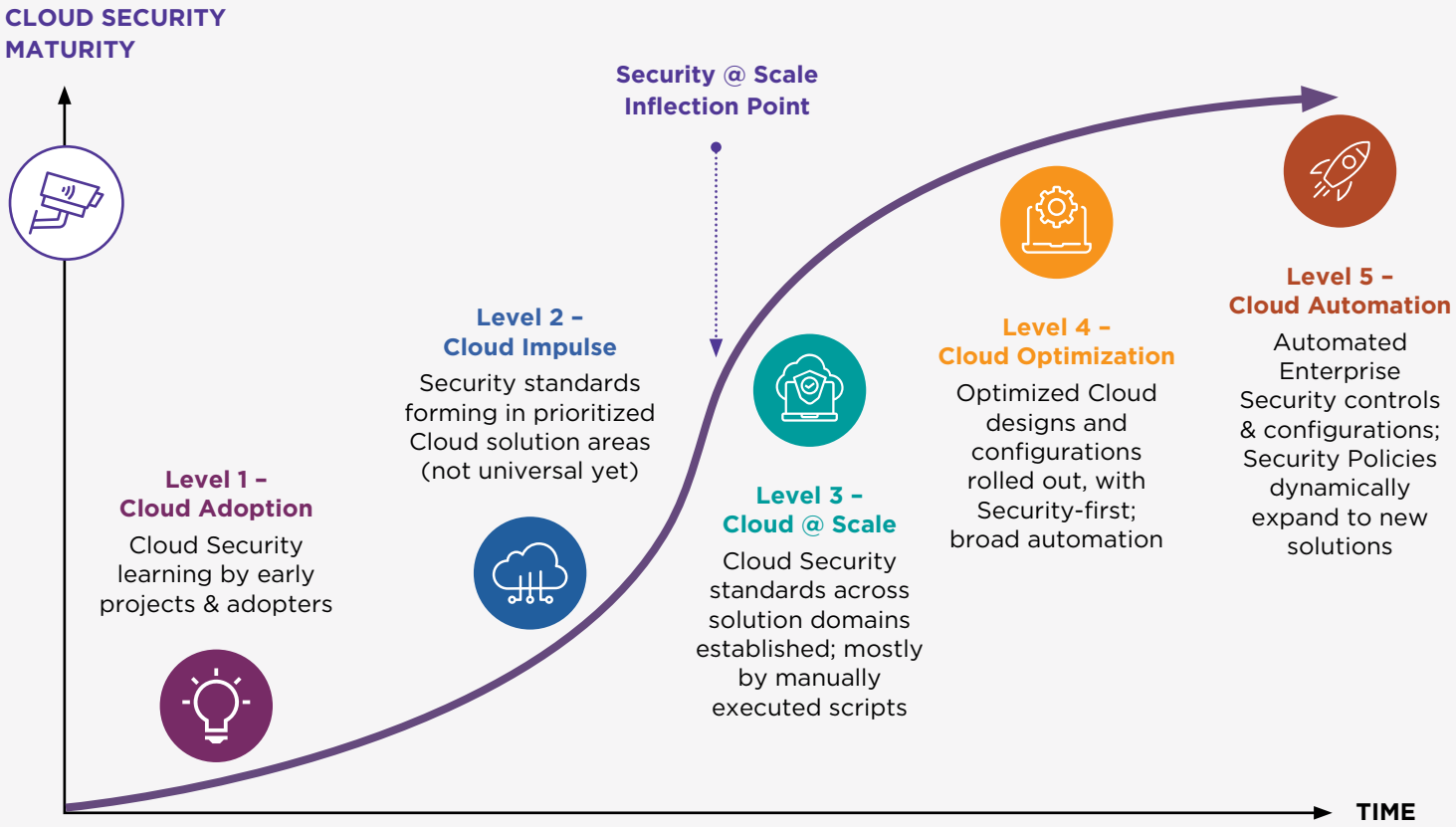


Diagram 2: Typical Cloud capabilities Maturity Model – Revisited to show progressive maturity levels for advancing Cloud Security capabilities via a Cloud Security Maturity Model (CSMM)

The levels we use for general Cloud capabilities maturity progressively are reused in the Cloud Security Maturity Model (CSMM) as we turn our focus on building your Cloud Security capabilities specifically. Note the general Cloud Maturity levels you probably have seen in the past – "Cloud Adoption", "Cloud Impulse", "Cloud @ Scale", "Cloud Optimization", and "Cloud Automation" (or something like this) – which identify progressive Cloud capabilities needed over time to gain consistencies and efficiencies, and optimization and automation opportunities, as we traverse each maturity level.

The same is true when applying these maturity levels to Cloud Security advancements, as you'll see when we detail progressive security improvements at each level:

Level 1 Cloud Adoption

- For overall Cloud Maturity: You are teeing up and learning from high priority, targeted projects, pilots, POCs, and early adopter teams to "get your feet wet" and learn "how to do Cloud" the right way, mostly from scratch
- For the Cloud Security Maturity Model (CSMM), it's also about experimenting and learning to –

1. Develop/Test and iterate early Cloud solutions with foundational Security requirements, controls, and early policies being formed
2. Benefit from early feedback to better (more proactively and robustly) secure next cycles of Cloud migrations and developed Cloud solutions
3. Teach your security team how to manage (manually at this stage) Cloud Security policies and procedures, mostly via the CSP console at this stage (no automation opportunities until you know more)
4. Define Security Architectures/Designs that mostly resemble previous on-prem solutions (e.g., server-based; focus on network perimeter, devices, and controls, etc.)
5. Initiate IAM for Cloud solutions, though ad-hoc for selected solutions at this stage, with little to no federation

Level 2 Cloud Impulse

- For overall Cloud Maturity: You are creating standards and economies within prioritized Cloud solution areas; and developing initial Cloud Operations processes and tools. This is foundational for potential reuse and refinement that leads to later Cloud @ Scale capabilities maturity.
- For the CSMM, you are prioritizing solutions, solution domains, and security requirements (based on business priorities) to build up your secure Cloud footprint; and learning to execute Cloud Security actions effectively (as a precursor to efficiencies) for these prioritized areas and solution types, to –

1. Define early reusable Cloud Security & SecOps policies, procedures, and tools for prioritized solutions and domains, including those to start building a layered defense strategy
2. Engage selected business and IT stakeholders, including owners for prioritized applications, solutions, data domains, and security requirements
3. Build early Cloud SecOps capabilities (e.g., observability, reports, dashboards, and underpinning processes and data management)
4. Identify and fill high priority Cloud Security skills and tools gaps for prioritized solutions, applications, and data protection needs
5. Initiate Infrastructure-as-Code (IaC) tools and processes usage for provisioning and environment consistency and reusability within prioritized solution domains. Across these, however, security designs may still be inconsistent with little to no reuse
6. Begin limited MFA design and usage (due to difficulties in supporting disparate teams and applications), with minimal federation

Level 3 Cloud @ Scale

- For overall Cloud Maturity: You are developing consistent Cloud standards, processes, and tools for enterprise-level adoption across multiple solution domains, including proactively incorporated requirements for planned solutions
- For the CSMM, you are transforming solutions for enterprise-wide Cloud Security efficiencies, and industrializing security designs, implementations, and SecOps processes and tools, to –

1. Establish Cloud Security policies and standards across multiple solution domains; still mostly enforced manually by executed scripts, but with growing emphasis on consistencies that lead to increased automation opportunities
2. Align the Cloud Security roadmap with the long-term Cloud strategy/capabilities roadmap and timeline, as an enabler for this, including further building your teams' expertise around a layered defense strategy
3. Transform earlier Cloud solution strategies and supporting security requirements (from inefficient IaaS approaches) to significantly more PaaS and selective SaaS designs with configurable, dynamic security controls and services
4. Advance Cloud solution migration and development planning and designs towards more proactive, built-in security rather than reactively overlaying an improved security implementation afterwards
5. Initiate a strategic, overarching Cloud SecOps Model to address current and planned needs for expanding Cloud solutions; including more robust defense layers to address an increasingly complex Cloud footprint (via maturing designs, policies, procedures, and tools usage)
6. Regularly use standard architecture and design reviews to jointly refine/reuse security designs and configurations
7. Build initial automation opportunities via scripted processes and serverless actions; create initial patterns for later reuse and increased automation scope

Before we proceed to detailing Levels 4 and 5 of the Cloud Security Maturity Model, it's important to note that the "Security @ Scale Inflection Point" (shown in Diagram 2) must be achieved before Cloud @ Scale capabilities are effective. Think of "Security @ Scale" as a prerequisite and enabler for accomplishing general, enterprise "Cloud @ Scale" capabilities and efficiencies.

Cloud Security – Guiding Principle #5:

Most organizations look to achieve Cloud @ Scale general maturity level and related economies, or better; however, these will only be effective when supported by previously established Cloud Security capabilities and efficiencies (ready for Cloud @ Scale as we transcend the Security @ Scale Inflection Point)

Level 4 Cloud Optimized

- For overall Cloud Maturity: You are now consistently rolling out and reusing pre-optimized Cloud designs and configurations, thus enabling broader automation opportunities for the Lifecycle, and CloudOps and SecOps
- For the CSMM, you are proactively optimizing Security-first solutions consistently for reusable Cloud security efficiencies and multi-layered defenses; and standardizing optimized security implementations and SecOps processes and tools to identify progressive automation options, to –

1. Standardize/Scale Cloud Security optimizations via a roadmap that (eventually) addresses all solutions types
2. Promote cross-teams' Cloud Security-first best practices, communications, and training
3. Utilize only secure Cloud-native best practices for all solution development; and optimize/reuse PaaS and SaaS security configurations (while minimizing IaaS inefficiencies)
4. Automate a security library for application & data solutions' design reuse, whether used for migration waves or new Cloud development
5. Federate Security configurations, controls, and MFA across most solutions (where practical)
6. Roll out a standard SecOps model across all Cloud solutions, and fine-tune your multi-layered defenses consistently across solutions
7. Optimize/Automate Security management and operations via a centralized Cloud Security platform, including consistent monitoring views, dashboards, alerts, automated actions, and reporting

Level 5 Cloud Automation

- For overall Cloud Maturity: You are automating Cloud migration and development toolchains as well as CloudOps tools and processes, including notifications/alerts and reporting/dashboards; these will increasingly scale for new and changing solutions, dynamically
- For the CSMM, you are now regularly automating enterprise security controls and configurations, and Security policies and procedures, which dynamically expand to secure your new and changing solutions, to –

1. Automate progressive Cloud SecOps processes for all solution domains (to an extent that is practical)
2. Automate scalable, optimized secure Cloud architectures and designs proactively from a central security library, used by all Cloud migration and development teams
3. Plan for (and regularly implement) all new and changing workloads, applications and data solutions' automations via a strategic capabilities (and automation) roadmap
4. Centrally manage Security configurations for all solutions, domains, and accounts
5. Proactively integrate security into all IaC environments throughout the Cloud Solution Lifecycle

Level 5 Cloud Automation (cont'd)

6. Build "Security-first" directly into the Cloud stack and best practices; proactively use these in all Cloud architectures/designs, provisioning tools, and progressive automations for implementation and operations
7. Federate security across all solution domains, toolchains, and IAM and MFA processes
8. Continually master optimal balance between robust multi-layered defenses and the efforts needed to build and manage this complexity

Building out a mature security posture in the Cloud can be seen as a journey, much like building your overall Cloud capabilities via a strategic roadmap. But in the case of Cloud Security, this should be managed as an enabling set of capabilities that need to be established before you can efficiently expand your overall Cloud capabilities. You really cannot accomplish efficient or accelerated Cloud solutions growth without first adopting these security enablers (see Guiding Principle #1).

It should also be noted that until you reach "Level 3 – Cloud @ Scale" capabilities, thus transcending the "Security @ Scale Inflection Point", you may be bogged down by manual, one-off, unscalable steps in your processes and tools usage. Graduating to (at least) this level of Cloud Security maturity will accelerate your journey towards security optimization and automation, in addition to the economies afforded to other Cloud capabilities on your strategic roadmap. Which brings us to Cloud Security GP #6…

Cloud Security – Guiding Principle #6:

Achieving higher levels of Cloud Security (scalable, optimized, or automated) requires a disciplined, pragmatic approach consisting of: a) Cloud Security-first mindset; b) continuous security improvements as part of your Cloud Operating Model (COM); and c) culture to extend security efficiencies via optimization and automation opportunities

BUILDING AND EXECUTING YOUR ORGANIZATION'S CLOUD SECURITY MATURITY MODEL (CSMM)

Such a pragmatic approach that promotes security capabilities to attain advanced maturity levels is introduced by the Cloud Security Maturity Model (CSMM; see Diagrams 3 & 4 below). Here, we provide guidelines and general definitions of what to achieve within each CSMM maturity level. However, you will need to further prioritize and detail the objectives of each maturity level to the specific cloud goals of your organization. Some activities and priorities can be planned and enacted on sooner or (slightly) later, depending upon your organization's objectives, roadmap, timing needs, and overall strategic Cloud capabilities roadmap.

For one example, depending on where you are on your Cloud journey, you'll need emphasis on the security implications of either Cloud migrations or Cloud-native development. If early in your journey, where cloud migrations are key to mass transitioning from your data center as a top priority, this will (of course) impact your near-term Cloud Security needs differently than if you have a more mature Cloud footprint where new solutions are continually introduced via Cloud-native development and optimization as a higher priority. Make sure you integrate the appropriate business and organizational strategic priorities into your Cloud Security planning and roadmap… because the right evolution of your Cloud Security capabilities will still be a prerequisite/enabler (or detriment) to your overall Cloud journey.

Similarly, for another example, depending on your organization's adopted solution design strategy (IaaS vs. PaaS vs. SaaS; and when, why, and how you utilize each), you will have different Cloud Security needs, activities, and efforts as you progress through the higher efficiency "Cloud @ Scale," "Cloud Optimization," and "Cloud Automation" maturity levels. Hence, build your organization's unique Cloud Security capabilities roadmap for your defined success; but you can start with the following CSMM definitions to initially guide you in planning your prioritized security capabilities development.

See Diagram 3 below to address the 1st three Cloud Security Maturity levels (culminating in the suggested minimal target maturity of "Cloud @ Scale" and surpassing the "Security @ Scale Inflection Point"). The CSMM will help you understand how the security activities of each maturity level interact with the Cloud Solution Lifecycle and its Phases discussed earlier. This gives you additional granularity in planning and executing your organization's unique Cloud Security capabilities roadmap; and can help you determine how and when to build out each security capability in a way that will support your specific adaptation of the Lifecycle.

For Organizational Cloud Maturity Level	1 Cloud Adoption Experiment & Learn	2 Cloud Impulse Prioritize & Execute	3 Cloud @ Scale Transform & Industrialize
For each Cloud Solution Lifecycle Phase	**Cloud Security Capabilities to enable progressive and secure Cloud Maturity:**		
1 Plan	a) Plan iterations of early Cloud solutions (migrated or new), incl. Security requirements, controls, policies b) Address project-specific cloud security reqts. c) Share learning, early feedback to plan security for new cloud solutions and types	a) Plan project- or domain-specific Security strategy and SecOps; not across accounts yet b) Engage selected (applications, data, security) stakeholders/ owners for strategic priorities c) Start filling Cloud Security skills & tools gaps based on prioritized solution domains, apps	a) Aligned Cloud Sec. roadmap with long-term Cloud capabilities roadmap; incl. further expertise for a layered defense strategy b) IaaS plans shift to planned PaaS services and Cloud Security controls/services c) Advanced plans/designs for built-in security
2 Setup/ Design	a) New, prioritized Cloud Security policies and procedures created b) No automation yet; manually configured policies and procedures (mostly via console) c) Security Arch/designs resemble on-prem (server-, perimeter-based; network controls)	a) Early Cloud Sec. & SecOps policies, standards, tools for prioritized solutions, layered defense b) IaC use (e.g., Terraform, CloudFormation) for simple provisioning automation, reusability c) Prioritized sec. designs addressed; not reused d) Security is inconsistent part of Design reviews	a) Security automation (scripted) and controls designed for most used solutions, domains b) Regular Arch/Design reviews uphold reused, effective cloud security designs, IaC usage c) Basic, consistent automation scripts (via serverless FaaS, Lambda, etc.)
3 Migrate/ Build	a) Benefit from early feedback to secure next Cloud Migrations or new Development targets b) Only ad-hoc IAM with little to no federation c) Early, prioritized security development skills, tools (for migrations and new development) d) Mostly DevOps + SecOps, not DevSecOps yet	a) Prioritized Cloud Security configuration/development skills and tools b) Limited, growing MFA use (some federation); difficulties supporting disparate teams, apps c) IAM processes/tools becoming consistent across solutions; incl. selected automation	a) Some designs for proactively secure solutions b) Standardized (and growing) automation; i.e., mostly scripted via serverless actions c) Federation on most accounts with widespread MFA; still gaps in consistent implementation d) Evolving CSP + 3rd Party tools orchestration
4 Test	a) Security testing skills, tools resemble on-prem b) No DevSecOps; security testing is reactive	a) Prioritized Cloud Security testing skills, tools b) Early DevSecOps processes, CI/CD pipelines	a) Cloud-centric Security testing skills, tools b) Consistent DevSecOps, CI/ CD, security tests

5 **Deploy**	Local, non-critical deployments (POCs, Pilots) to learn, instead of large production solutions	Selected small to medium-sized production solutions; early critical (secure) deployments	Production (all solutions) prioritized by strategic business need, not Deploy capability
6 **Monitor**	a) Basic, small footprint (growing) to monitor b) Learn new cloud monitoring tools, processes	Common SecOps monitoring processes, tools; observability dashboards, logs, traces, metrics	Scaled SecOps monitoring, intelligence; ML, AIOps, Event Mgmt, anomaly detect/prevent
7 **Manage/ Operate**	Manual, project-based; not repeatable Cloud SecOps Model yet	Initial SecOps model, processes established across apps, domains (incomplete, growing)	Enterprise Cloud SecOps model, 1st iteration, refined and scaled for all solutions, domains
8 **Optimize**	Small solutions, not optimized (security, etc.) until this post-Deployment Phase (all reactive)	Continual optimizations improve upon designed/built-in solution optimizations	Post-Deploy optimizations lessen as improved built-in solution optimizations prevail

Diagram 3: Defining the Cloud Security Maturity Model: Levels 1 through 3

For completeness, the details above show many significant aspects of each CSMM level across each CSL Phase. Use this cross-reference to proactively plan for when defining and building your processes, roles, and tools usage that each of these maturity concerns should be addressed (i.e., have impacts).

Note the transition from manual, ad-hoc processes and tools in early maturity levels to more consistent, repeatable, and reusable capabilities as you transcend the "Security @ Scale Inflection Point" to achieve "Cloud @ Scale" maturity. You are gaining economies and efficiencies with each maturity level. Another trend is the increasing scope of solution types and domains as you gain confidence in Cloud capabilities, thus reinforcing the need for consistency and reusability to handle this growing volume and potential diversity. These trends for increasing efficiencies and scope will continue throughout the "Cloud Optimization" and "Cloud Automation" maturity levels as you'll see.

Transcending the "Security @ Scale Inflection Point" – Cloud Economies Gained

Security @ Scale is necessary to provide security for Cloud @ Scale advancements – you can only securely optimize or automate efficiently with such security capabilities that scale for broader cloud economies and accelerated growth, including:

- Provisioning processes and tools, including secure IaC patterns for reuse in standing up consistent infrastructure instances, core services, and environments
- Increased PaaS-based solutions, including configurable, self-administering services, auto-scaling, etc., in lieu of decreasing IaaS solutions
- Converged, consistent best practices and tools (securing both migrations and development), including centrally managed policies, procedures, configurations, and controls
- Consolidated, centralized, single security management platform

Security @ Scale Inflection Point = Reached Cloud Security maturity and efficiencies that seamlessly (no significant security concerns) enable Cloud @ Scale (and beyond)

- You've achieved the means to efficiently expand and scale security dynamically along with your growing Cloud footprint
- Cloud solutions expand and scale (for applications and data, whether migrated or developed) and are intrinsically linked to mature security processes, and tools

Hence, as overall organizational cloud maturity progresses, Cloud Security will proactively support and easily scale to your evolving Cloud footprint

- This support paradigm was established earlier (proactively) via a Cloud Security-first strategy and culture
- Including a growing scope of applications, data, services, infrastructure, and network components

From Scaled efficiencies to Optimized and Automated acceleration of our Cloud journey!

Also note that the CSMM as a tool for your Cloud Security planning can be utilized in different ways, depending where you are on your Cloud Security journey:

1. **For a Cloud Security maturity assessment**

   You may do this initially, or periodically, to see where you are versus where you should be; and to develop the relevant next steps to achieve your target level of maturity for a specific product line, solution domain, business unit, or rolled up for an enterprise-level Cloud Security maturity assessment

2. **For Cloud capabilities roadmap planning**

   Whether part of overall Cloud capabilities planning (with security designed-in to lead and enable other Cloud capabilities), or planning for a more Cloud Security focus on advancing capabilities

3. **For a starter Cloud Security checklist**

   To assist any particular Cloud Security-related program or project; and ensure it is achieving its security objectives, and help define how to remediate (via gap analysis) if it isn't meeting these

Cloud Security – Guiding Principle #7:

Establish an appropriate Cloud Security Maturity Model (CSMM) for your organization's unique Cloud journey and cloud capabilities development, including:

a) Integrate this into your overall Cloud Strategy and capabilities roadmap, as well as your solutions lifecycle; and

b) Realize the multiple ways to refine and utilize your adopted CSMM in support of Cloud Security related programs and projects throughout their lifecycles

See Diagram 4 below which addresses the activities to accomplish the two remaining (advanced) Cloud Security Maturity levels. Here, you will be improving upon your mature (consistent and efficient) policies, procedures, processes, and tools usage towards even better business outcomes. Optimizing your Cloud Security capabilities for Level 4 maturity implies that you are achieving the highest levels of (practical) efficiencies; then, combining this with standardized ways to achieve such efficiencies, you can now automate such processes and tools as part of Level 5 maturity.

Finally (for long-term success), to regularly support the retention of these highest Cloud Security maturity levels, you will also master your Cloud Security governance and change management in Level 5 maturity. At this level, such governance becomes increasingly important to ensure you don't backslide or break any previously achieved cloud optimizations or automations while your cloud footprint continues to evolve.

For Organizational Cloud Maturity Level	4 Cloud Optimized Optimize & Standardize	5 Cloud Automation Automate & Govern
For each Cloud Solution Lifecycle Phase	**Cloud Security Capabilities to enable progressive and secure Cloud Maturity:**	
1 **Plan**	a) Standardize/Expand/Scale optimized Cloud Security via strategic Cloud roadmap and pragmatic governance b) Promote cross-teams' Cloud Security practices, training, knowledge sharing, and communications (accelerated via growing collaboration)	a) By default, plan security automations across all new or redesigned workloads, data solutions, and applications; rare when a solution cannot achieve at least minimal, standard security automation capabilities b) Cloud Security-first culture drives cross-team collaboration, efficiencies
2 **Setup/ Design**	a) Solutions designed proactively for secure Cloud-native build practices b) Further expanded reference library of automation design options; and automation extends to policies/ procedures that span multiple accounts c) Only design for IaaS when unusual solution, tech stack, or contract isn't amenable to pursuing more modern architecture/design options	Build enterprise-wide Cloud Security Governance to: a) Regularly reuse and automate secure Cloud designs from shared library b) Dynamically integrate Security in all new, changing IaC environments) Continually master balance between multi-layered defenses and effort to build and manage complexities

3	**Migrate/ Build**	a) Use secure Cloud-native development practices, tools, services b) Configurable, scalable, self-administering PaaS services prioritized over IaaS in execution, skills-building c) Automate Security library for apps' & data solutions' design reuse d) Standardized federation and refined Security configurations/controls across solutions, domains (incl. MFA); some gaps supporting toolchains e) Shift from manually created/executed (scripted) security automations to managing/running automation via central platform, incl. reporting	a) Built-in Security-first principle into Cloud stack and shared designs for both solution provisioning and automations b) Predominantly automated, auto-scaled, self-administered PaaS services (diminishing IaaS to manage) c) Consistently designed and applied Cloud-native development best practices, tools, and services d) Optimized and automated standard federated Security across all solutions and domains (incl. MFA, toolchains)
4	**Test**	a) Refined Security testing skills, tools used across all solution, domains b) Advanced DevSecOps processes & tools, CI/CD pipelines, security tests	a) Standard Security testing (incl, automation) skills, tools across solutions b) Optimized DevSecOps processes, tools, security test suite automation
5	**Deploy**	Rollout Cloud SecOps model across solutions; fine-tune layered defense	Automate Enterprise Cloud SecOps model as practical across solution
6	**Monitor**	Refined Cloud SecOps observability, actions - effective reports, active recommendations, dashboards, incident resolution via service Bots	Automated enterprise Cloud SecOps monitoring, actions; incl. Bots for security recommendations, service fulfillment, running scheduled tasks
7	**Manage/ Operate**	a) Enterprise Cloud SecOps model (1st iteration) established; refined and scalable across all solutions, domains b) Standardized upfront security optimizations, progressively automated and managed via a centralized Cloud Security Platform	a) Highly automated Cloud SecOps processes, configurations, monitoring, notifications, remediations (growing as much and as quickly as practical) b) Centrally managed (platform) Security configurations, controls, policies, and procedures for all solutions, domains, and accounts
8	**Optimize**	Post-Deploy optimizations lessen as improved built-in solution optimizations prevail	Post-Deploy optimizations only occur in unplanned solution change management (i.e., original optimal design must change for new circumstances)

Diagram 4: Defining the Cloud Security Maturity Model: Levels 4 – 5

Note that in traversing these advanced Cloud Security maturity levels, you will drive continued improvements beyond the scalable and efficient security processes and tools gained by "Cloud @ Scale" maturity (and having surpassed the "Security @ Scale Inflection Point"!).

Therefore, the key objectives of CSMM levels 4 and 5 are to:

1. Further address enterprise-wide cloud solutions' scope and scale, including –
   - / Security across all solution domains, business units, and Cloud accounts
   - / Enterprise-level consistencies and reuse of security policies, configurations, designs, controls, and monitoring

2. Build enterprise-wide security efficiencies and standardizations to enable –
   - / Standard security optimizations that will be part of the reusable, highly efficient patterns
   - / Progressive automation opportunities that are identified to bring optimized processes and tools usage to the next level of efficiency

3. Develop enterprise-wide Cloud Security Governance processes, roles, and cadence, including –
   - / Applied best practices for consistently developing and reusing optimized Security policies, configurations, designs, controls, and monitoring
   - / Governance cadence and incident management processes to drive security continual improvement and remediations within a security optimization and automation framework that supports the Cloud Security capabilities roadmap

In addition to these key objectives, you'll notice several important trends that will emerge as part of these advanced Cloud Security maturity levels:

Cloud Security-first culture will be sufficiently established to drive regular cross-organizational collaboration, and shared efficiencies and improvements

Reuse of optimized Cloud Security designs from a shared library will be frequent and automated where possible

All IaC environments will proactively and dynamically integrate Cloud Security best practices

Monitoring and governance activities will continually master an optimal balance between multi-layered defenses and the increased effort needed to build and manage this complexity

Automation Bots will be increasingly employed for –

a) Refined Cloud SecOps observability and actions, including recommendations generation and dissemination and incident resolution
b) Automated enterprise Cloud SecOps actions, including (security, etc.) service fulfillment and running scheduled tasks

A single centralized Security platform will be established and adopted; capable of managing all policies, configurations, controls, and automation levers across all solutions, domains, and accounts

BUILDING CLOUD SECURITY INTO YOUR ORGANIZATION'S CLOUD OPERATING MODEL

If your overall cloud strategy, progressive capabilities, and proactive security needs are jointly managed via an aligned, comprehensive cloud roadmap (as we'd recommend), then a cross-organizational Cloud Operating Model (COM) is key to orchestrating these Cloud Security maturity levels holistically for the organization's goals, priorities, and as continual enablement for your other cloud advancements.

Your most important cloud strategy objectives cannot be fully realized without following the Cloud Security Guiding Principles for a strategically aligned Cloud Security roadmap (see all 9 listed this strategy brief, which should be incorporated into your COM).

Cloud Security – Guiding Principle #8:

Well-defined and established Cloud SecOps as part of your overall Cloud Operating Model will ensure your organization's Cloud Security standards, best practices, processes, efficiencies, and automation levers are executed effectively across all solutions and projects for long-term, secure Cloud Strategy success

There are two sides to this. As part of your overarching Cloud Strategy, and managed within your COM, following this Guiding Principle will:

- Guide creation and maintenance of an effective Cloud Security roadmap for continual alignment with your organization's priorities in rolling out strategic Cloud capabilities
- Ensure completeness of your Cloud Security capabilities at any given time for strategic programs, projects, and solutions to support your organization's unique Cloud journey

At a high level, there are 4 key areas where combined Cloud Strategy/Security benefits come into play – to be defined early for execution within your Cloud Operating Model:

Optimal Cloud Security organization and skills

Secure Cloud Migrations (with minimal deferred rework)

Proactive, efficient (including high reuse) new solutions development via optimized security designs, and progressive security automation

Centralized Cloud Security management and support

You can see that each of these benefits naturally spans broad areas of organizational, process, and technology guidance to grow and mature your Cloud footprint in a secure manner.

CLOUD SECURITY IMPLEMENTATION BEST PRACTICES

While previous discussion revolved around strategic-level decisions and practices to shape your overall Cloud Security organizational and process maturity, we will now further address key details in implementing strong Cloud Security for your solutions. These will be particularly helpful in areas where your teams are initially less knowledgeable, as hints on where to get started. We explore 10 overall Cloud Security implementation best practices.

We divide these Cloud Security Implementation Best Practices into 3 main areas – foundational ("plumbing") concepts (best practices 1-4), IAM considerations (best practices 5-7), and advanced topics (best practices 8-10). See Diagram 5 below for four best practices of "Foundational Plumbing" implementation advice.

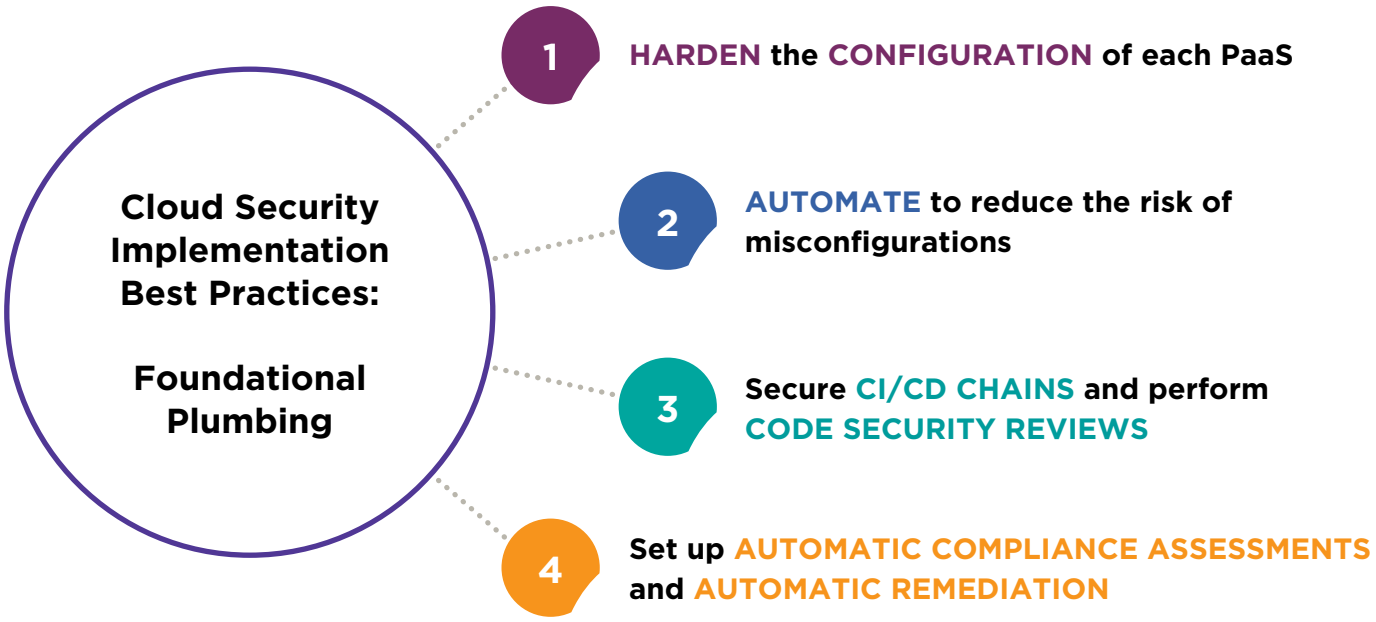


Diagram 5: Cloud Security Implementation Best Practices: Foundational Plumbing

Looking at the 1st Cloud Security implementation best practice to harden the configuration of each PaaS service; and understanding that PaaS designs and configurations will likely be an increasingly important part of your cloud landscape (perhaps progressing from earlier IaaS migrations), then all such services should become security hardened over time. You'll want your Cloud design and implementation teams to become skilled in developing and configuring all relevant PaaS services your organization adopts to be proactively secure and reusable across new solutions.

In hardening your PaaS services configurations:

Prepare a cloud risk assessment for every service to be consumed
/ Agility is key; be flexible as new solutions may utilize a service differently
/ Review the analysis regularly (i.e., whenever deploying a service for a new solution or release)
/ Note the most relevant service for a particular need may change (either the choice in service or a particular configuration)

Identify all available security parameters that can reduce the risks of each service; those of the service itself, but also other related cloud configurations that affect the service
/ Cloud providers continue to evolve their services, and they will add new services regularly
/ Stay aware of services evolution within your solutions requirements and design

Specify security configuration requirements in relation to how (and how much) the service will be used
/ There is no one-size-fits-all solution, and configurations may need adjustment as related processes or volume of usage changes

The 2nd Cloud Security implementation best practice is to automate (in multiple ways) for the purpose of reducing the risk of misconfigurations. In short, wherever there are repeatable patterns of design/configuration, there is potential for automation to be considered (and likely implemented); and once you've perfected (secured, etc.) a particular configuration, make sure you always do it in that optimized way. Automation implies systematic reuse and propagation of something we already know to be defined well and configured correctly and securely, whether it's a service, process, type of resource, etc.

Here are some ways you can automate to reduce risk:

Develop and manage design and code security configurations in deployment templates; and provide reusable secure-by-design architectures

Secure deployment in UAT environments before production; and disallow any such configuration changes directly in production (must go through UAT in code promotion)

Significantly reduce human errors in CloudOps; adopt an "automate everything" culture for security, etc.
/ As little as possible (striving for zero) administration in production environments to reduce misconfigurations after deployment (or illegitimate accesses)

The 3rd Cloud Security implementation best practice is to secure your CI/CD chains and perform regular code security reviews. This includes:

Secure your chains at all levels (process, services, objects, and code)

Utilize tools to control CI/CD from one solution development/deployment to another (e.g., Checkmarx, TFSec)

Ensure that DevOps is advanced into well-integrated DevSecOps for your teams, in both skills and culture

- For all related processes, tools, and expertise; including skills in agile teams with security champions and progressive training
- But acknowledge that tools will never replace skills (i.e., only automates and amplifies the skills of your team)

The 4th Cloud Security implementation best practice, and the final one we address amongst foundational concepts, is to establish automatic compliance assessments and remediations whenever possible. This includes:

Go native and use Cloud Provider services to monitor logs and trigger alerts

- Don't forget to dedicate accounts and subscriptions specifically for log management and security treatments
- Perhaps augmented by 3rd Party tools to consolidate and analyze information

Implement automatic remediation for selected non-complex patterns

- e.g., PaaS public exposition; there's no need to mobilize people to click on the "private" button

The next area of Cloud Security implementation best practices we'll explore are those around Identity and Access Management (IAM) considerations, clearly of utmost importance in securing your cloud, etc. environments, solutions, and data.

See Diagram 6 below for three best practices of “IAM Considerations” implementation advice.

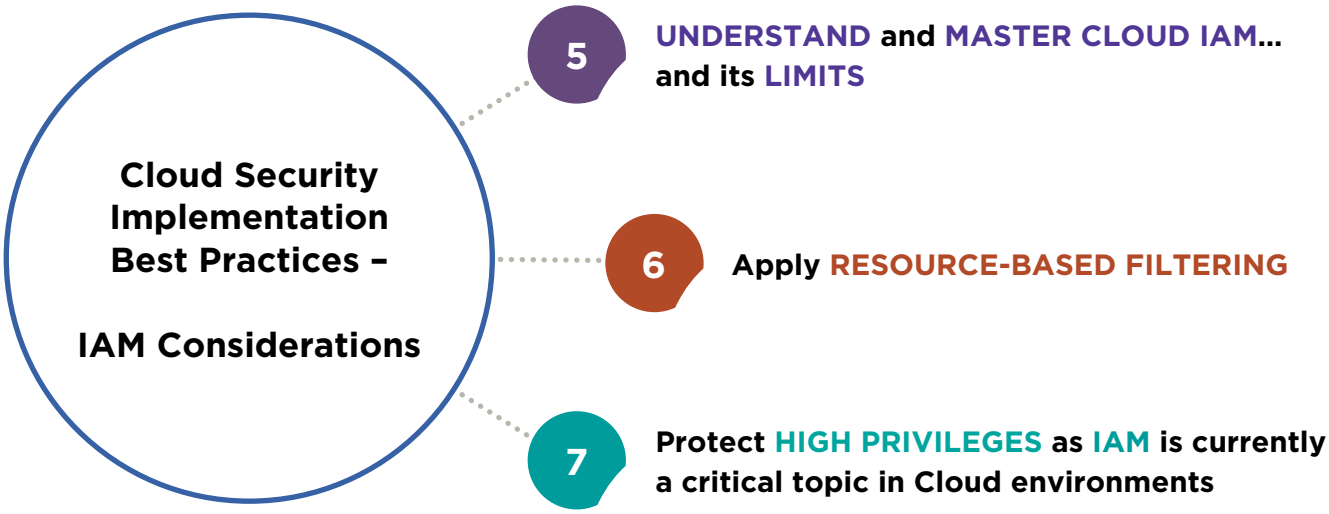


Diagram 6: Cloud Security Implementation Best Practices: IAM Considerations

The 5th Cloud Security implementation best practice is to understand cloud IAM capabilities and its limitations, and to master these as part of IAM-driven risk management. See Diagram 7 below for an overview of cloud IAM understanding and general considerations.

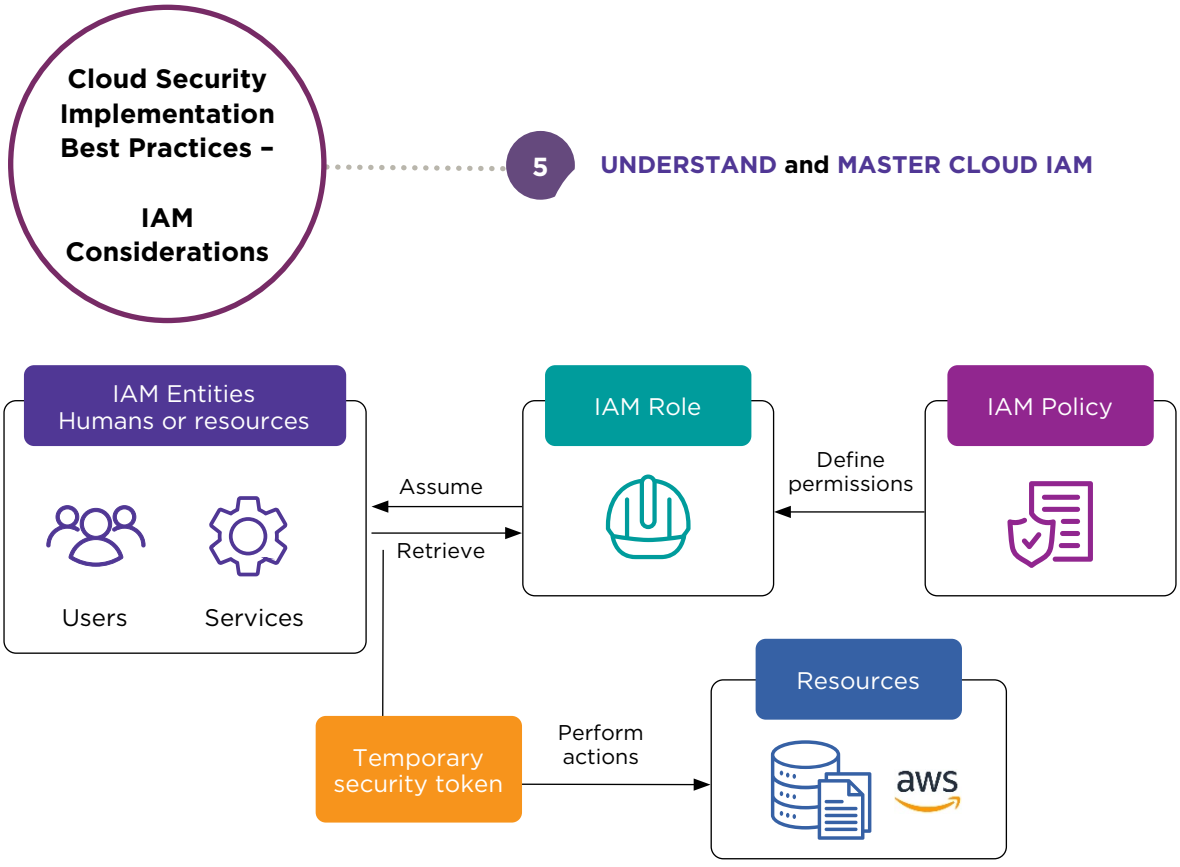


Diagram 7: Cloud Security Implementation Best Practices: Understanding Cloud IAM

Some highlights to take from Diagram 7 to understand cloud IAM:

Develop robust IAM policies that span all relevant cloud solutions' processes and users (all types); and covering all related IAM entities and roles

Enforce two primary security rules universally when handling IAM in the cloud –

- / Give only necessary IAM entities the authority to assume certain roles, particularly those with higher levels of access
- / Follow the "Principle of Least Privilege" in a Roles-Based Access Control (RBAC) model. Implementing both aspects of this rule (least privilege and RBAC) is best practice in any enterprise, but cloud and its potential exposures and costs related to IAM "ups the ante" for this stronger model

Depending on the policy, restrict access (or even specific actions) at the resource level rather than by domain or process (as needed)

Note that while this is an AWS view, most concepts remain consistent with Azure and GCP as well. However, mastering AWS IAM also requires an understanding of its limitations; while it's still necessary to follow the principle of least privilege (restricting access to minimal resources), this may not always be possible in AWS.

Typically, in AWS up to 46% of privileges cannot be restricted in terms of resource-level. For example:

- On Lambda (serverless computing) – From the moment you give even "List Functions" access to an entity, you implicitly give that person/resource the right to list all the lambda functions of the account
- It's even worse on the EC2 service where more than 75% of privileges cannot be controlled at the resource level. To restrict such access to resources, you are forced to use other AWS services to fill the "IAM gaps" –
  - / Such other services make it possible to tag resources and therefore create resource clusters of the same application/solution scope or sensitivity
  - / Then, Security Control Policies can further control access as overloaded access policies (at the organization level); e.g., restrict all access to the built-in root account of each AWS account

The limits presented here are only AWS, but other gaps in access restrictions exist amongst Cloud Provider services. Make sure your IAM team, as it takes on the cloud platform(s) of choice, becomes well-versed early in developing the appropriate IAM strategies, policies, and configurations for your cloud solution landscape.

The 6th Cloud Security implementation best practice is to apply resource-based filtering, incl.:

Create Security Groups in addition to traditional North-South (DMZ) filtering
/ Deploy access policies at the object-level – instance, container, database, bucket, etc.

Let the "IT business" and process/application owners focus on access rules for business objects rather than IT resources
/ Facilitate secure process flow management with business- and domain-level objects (e.g., Web Server, Database, Gateway, etc.); automate implementation filtering rules at the appropriate level(s)
/ It's up to the IT expert security practitioners to translate as needed to resource-level controls

The 7th Cloud Security implementation best practice is to protect high privileges (i.e., traditional Privileged Access Management – PAM) via IAM (and perhaps other defense layers); currently a critical topic within the cloud community. Providing such PAM controls includes:

Use your Cloud Provider's IAM boundaries and controls intended to restrict privilege escalation
/ e.g., while primarily via IAM boundaries in AWS, you can utilize the Contributor role in Azure

Apply 3rd Party tools to dynamically analyze your IAM configuration and provide guidance
/ IAM scanning modules regularly detect and report on the most privileged cloud entities (e.g., SkyArk)

Establish active MFA for all Admin accounts
/ MFA is generally native (or a well-integrated 3rd Party tool) and a free option; you really have no reason not to implement this important control

We now move on to the final area of Cloud Security implementation best practices. Here, we'll explore a few advanced topics to pay attention to as you build out your (secure) cloud footprint, including vulnerability management, monitoring and response, and critical data protection.

See Diagram 8 below for three best practices of "IAM Considerations" implementation advice.

Diagram 8: Cloud Security Implementation Best Practices: Advanced Topics

The 8th Cloud Security implementation best practice is to reconsider your approach to vulnerability management when in the Cloud. The main point here is one we brought up earlier in this strategy brief (see Guiding Principle #2) around the need to plan for and build out a layered defense; and with the additional controls at multiple levels that you can configure in the Cloud, you just need to:

> Do this proactively, in advance of any new domains or solutions where particular layers make sense; your security and development teams will partner on this point

> Continue to build this out more robustly over time, as additional layers/services/tools become available; your security team should recommend (via communications, policies, and designs) appropriate layers per solution type and/or security rating

The 9th Cloud Security implementation best practice is to continually increase your cloud observability, awareness, and efficiency in response. You now have better tools and data to do so in the Cloud than you ever had on-prem. Be sure to:

> Utilize Cloud-native SIEM services that are capable of dynamically detecting the theft of credentials
> / e.g., AWS GuardDuty integrates this service into others, and Azure does the same with its Security Center

> Automatically deactivate unused or suspicious IAM accounts
> / Linking this detection to other Cloud Provider services, so to proactively exterminate any emerging threats

The 10th, and last, Cloud Security implementation best practice is to understand and plan for your critical data resources now residing in the Cloud. Start with the premise that every organization is vulnerable, even when in the Cloud; therefore, you must plan accordingly for protection as well as remediation, including:

Protect high privileged accounts (of course), but have a plan for their breach

/ Establish a labelling strategy that is associated with global restriction policies
/ Regularly monitor for any unusual behavior that could expose a breach early in progress
/ Be ready to shut down and quarantine accounts or services that may become compromised by such a breach

Design and implement an enterprise cloud resilience and backup strategy

/ For your organization's necessary coverage of applications'/solutions' data domains, security classifications, and related recovery time objectives (RTOs) and recovery point objectives (RPOs) to be achieved in the case of compromise
/ Separate resource groups and dedicated accounts (or organizations) up or down to appropriate granularity for control and remediation

Again, these selected implementation best practices are intended to complement the strategic priorities and activities of the progressive Cloud Security maturity levels discussed earlier. Refer to these lower-level actions as needed to get started in key areas where your teams may be immature; but always ensure you are serving the greater good towards increased levels of cross-teams, processes, skills, and tools maturity for your organization's unique cloud journey.

CONCLUSION AND NEXT STEPS – MANAGING CLOUD SECURITY MATURITY

Whether you're just embarking upon your Cloud journey and migrations or have completed multiple migration waves and are now developing new or improved solutions in the Cloud, knowing how to proactively secure your organization's unique cloud footprint is critical to your cloud strategy success. If you move significant workloads insecurely to the Cloud and try to secure these later, as some organizations have tried, you are likely going to wish you addressed security more proactively.

The following are some key takeaways from this Cloud Security strategy brief; hence, to get started with your organization's unique Cloud Security strategy and capabilities building, our experts at Wavestone offer these steps:

1 Develop an appropriate Cloud Security Maturity Model (CSMM) for your organization

- / Use it as a Framework to help level set the Cloud Security conversation within your organization
- / Utilize the CSMM in different ways to guide strategy adjustments throughout your organization's Cloud journey and solution lifecycle
- / Pay particular attention to CSMM interactions with your adopted Cloud Solution Lifecycle (CSL) and solution design strategy (i.e., IaaS vs. PaaS vs. SaaS, all combinations, and when/why)

2 Build Cloud Security capabilities proactively aligned with your Cloud Strategy

- / You cannot be strategically successful in your long-term Cloud journey without early and continual Cloud Security optimization
- / Risks you incur otherwise would eventually break critical applications and data

3 Apply Cloud Security Guiding Principles to pragmatically mature your Cloud Security best practices (see details for each GP provided earlier in this brief)

1) Acculturate a Cloud Security-First as an overarching, desirable GP throughout the Lifecycle and Maturity curve
2) Build a layered Cloud Security strategy and supporting defenses
3) Plan and Design Security proactively into your Cloud solutions in early Lifecycle activities
4) Refine and enact Cloud Security throughout the Solution Lifecycle; and note that Cloud Security will be most mature in organizations that:
   a) Shift solution security actions to earlier Lifecycle Phases; and
   b) Employ an agile DevSecOps approach to all solutions

3 Apply Cloud Security Guiding Principles to pragmatically mature your Cloud Security best practices (see details for each GP provided earlier in this brief) (cont'd)

5) Achieve Cloud @ Scale general maturity level and related economies or better; but note these will only be effective when supported by already established Cloud Security capabilities and efficiencies (transcending the Security @ Scale Inflection Point first)
6) Reach highest levels of Cloud Security maturity using a disciplined, pragmatic approach and applying:
   a) Cloud Security-first practices;
   b) continuous security improvements via a COM; and
   c) culture to extend security efficiencies to optimization and automation
7) Establish a CSMM for your organization's unique Cloud journey and cloud capabilities development, incl.:
   a) Integrating it into your overall Cloud Strategy and roadmap; and
   b) Realizing many ways to utilize the CSMM in Cloud Security related programs and projects
8) Well-defined, established Cloud SecOps within your COM ensures Cloud Security standards, best practices, processes, efficiencies and automation levers are executed effectively across all solutions and projects for long-term, secure Cloud Strategy success

4 Align your Cloud Security (enterprise-, application-, and solution-level) with organizational business goals

/ A leading factor in establishing and repeatably applying the best security practices to your growing Cloud footprint is that your designs are aligned with your organization's planned capabilities
/ These must also be strategically represented in enterprise-level, application, solution, and data designs; and, hence, in implementation requirements
/ Building a reusable security-optimized designs library early will also ensure consistency, efficient reuse, and acculturation of proactive security incorporation

5 Optimize your Cloud Security to optimize your Cloud Strategy

/ Many organizations "back into" a Cloud Security strategy limited by designs and practices previously mastered for on-prem IT footprints; yet Cloud Security options for design, configuration, and monitoring provide more robust and efficient security controls to choose an improved strategic approach to security
/ This further enables overall cloud capabilities and Cloud SecOps efficiencies; think of Cloud Security as a worry-free accelerator for other cloud capabilities. For example, increased levels of centralized Cloud Security visibility and management will enable your teams to develop their business-level security optimization model that balances appropriate target security with costs and efficiencies
/ Improved security transparency, coupled with maturing security designs and processes, can add to your competitive advantage in the marketplace

6 Refer to the Cloud Security Implementation Best Practices presented earlier for additional detail in immature areas (to build up key areas of expertise)

So, do you need a Cloud Security strategy? By now, you should understand the value for any business "in the Cloud" to have a strong Cloud Security strategy, and to a large extent it should be aligned proactively with your overall Cloud Strategy. How large an extent depends on your unique business model and goals. It will generally not be about whether you secure your cloud workloads, but rather what is the right balance of security optimization (across different solution types, processes, and technologies) and related costs. Security starts with your organization's culture, where we suggest cultivating a Cloud Security-first approach. Dealing with this upfront in every design and process will only accelerate secure solutions going forward. In any case, security should be pursed as an early priority of your Cloud Strategy and improved upon (e.g., with a robust layered defense approach) continually from there.

A lack of Cloud Security maturity will make building a large Cloud footprint more difficult to plan and execute without introducing untenable risks. As your business continues to grow and rely on the Cloud to assist your digital transformation or product development efforts, having a strong Cloud Security roadmap of capabilities to continually secure your evolving cloud solutions and their target architecture/designs, to ultimately make your business more securely efficient, effective, and adaptable.

As you consider your organization's next steps to benefit from strategic Cloud Security capabilities and optimization, here are a few ways that Wavestone can immediately assist you:

01 Build a customized Cloud Security strategy with security posture planning, development, and maintenance for your organization and solutions

02 Transform your Enterprise IT Security teams and capabilities for an emerging Cloud-first strategy

03 Enhance your overall Cloud Strategy or Operating Model with security built-in capabilities and trajectory

04 Expand your Cloud Operating Model with increasing Cloud Security optimization capabilities and opportunities

05 Baseline and grow your Cloud Security maturity level and strengths across solutions and the organization

06 Develop a customized Cloud Security capabilities roadmap that addresses all organizational, processes, and technology considerations holistically; to build out your Cloud Security maturity to target levels in key areas

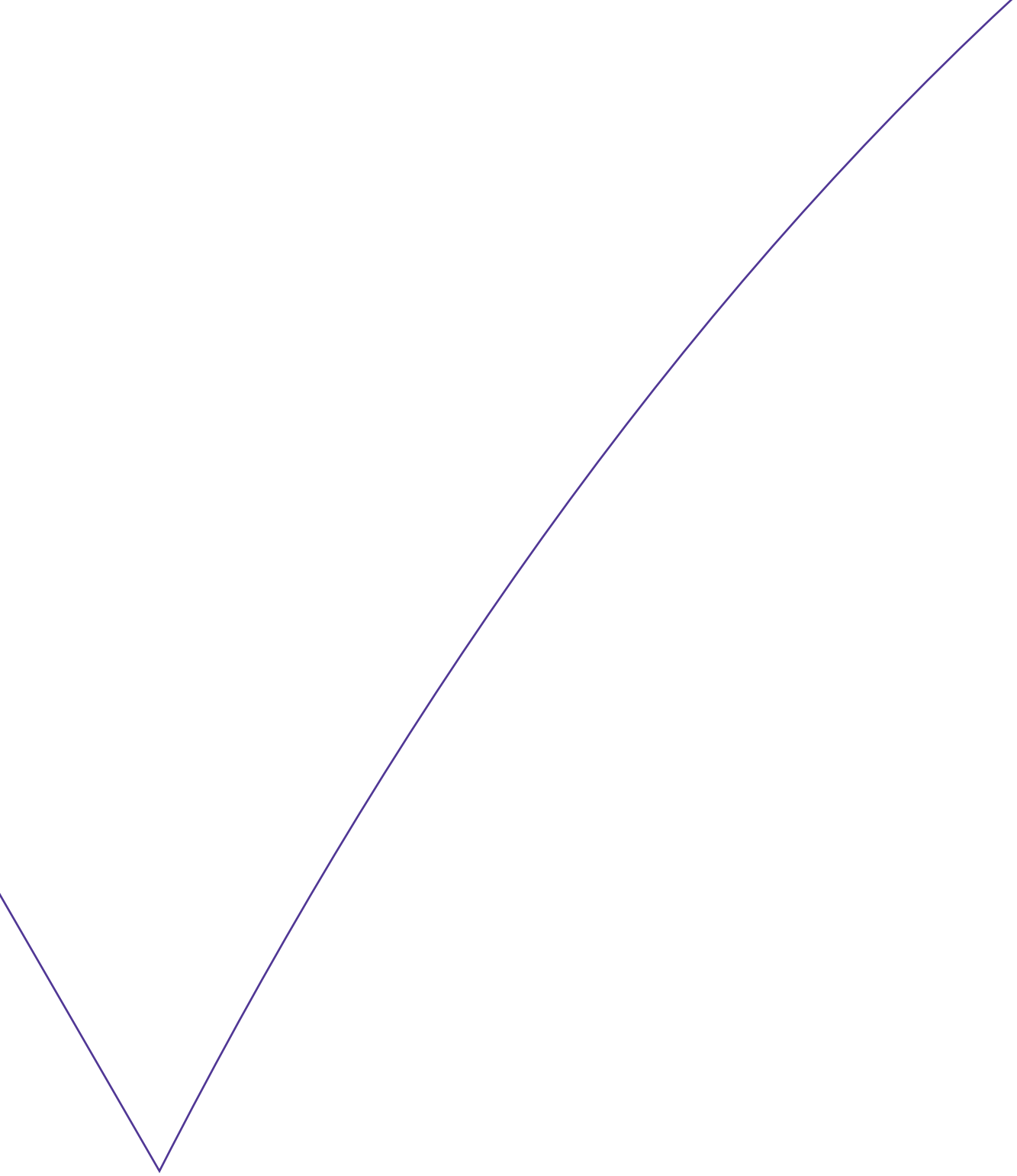
Feel free to reach out to us if you'd like to discuss your Cloud journey with optimization capabilities and opportunities and how to achieve optimal success.

About Wavestone

Wavestone is a business and digital consulting firm that supports organizations in delivering their most critical transformations. Over the past two decades, Wavestone has championed the transformations of more than 700 of the world's largest enterprises from a wide range of industries. Behind these successes is our ability to bring a winning mix of extensive hands-on experience, powerful analytical skills, and creative problem-solving to address our clients' greatest challenges. We drive change for growth, lower cost, and risk, and create the trust that gives people the desire to act.

WORLD'S BEST MANAGEMENT CONSULTING FIRMS | Forbes 2022 POWERED BY STATISTA

Forbes Names Wavestone among World's Best Consulting Firms 2022



The Positive Way

WAVESTONE

www.wavestone.com

In a world where knowing how to drive transformation is the key to success, Wavestone's mission is to guide large companies and organizations in their most critical transformation projects, with the ambition of a positive outcome for all stakeholders. That's what we call "The Positive Way".

Wavestone brings together 4,000 employees across 9 countries.

It is a leading independent player in the global consulting market,.

2023 I © WAVESTONE