sonraí SECURITY

WHITE PAPER

Charting a Cloud Maturity Journey

A Guide for Prioritizing Security Initiatives

The public cloud market is experiencing massive growth. According to ***Gartner***, public cloud spend will increase by $$482 billion in 2022 as companies continue to invest in emerging technologies — like virtualization, IoT, containerization, and edge computing — and increasingly leverage cloud resources to enable remote work.

That spend is being spread across multiple providers. Nearly half (48%) of organizations have a multi-cloud strategy in place. In fact, companies today use an average of three different cloud service providers (CSPs), while 28% use four or more.

While cloud computing eliminates capital expenses, reduces operational costs, and enables rapid entry into global markets, it also highlights new risk areas like security misconfigurations, weak data governance, poor identity and access management (IAM), and inadequate monitoring and reporting, to name a few examples. Critically, these risks tend to multiply in multi-cloud environments.

The scale and complexity of cloud infrastructure means that there will be a long list of controls to implement. Simplification via blanket policies for all environments will not work, as they will be both unenforceable and slow down the business.

A context-based and prioritized maturity journey is necessary to map the right policies to the right environments, and give the security team the right tasks at the appropriate time.

Read on to learn how to calibrate maturity goals across your cloud environments, and what policies are most important to start with.

What is Cloud Maturity?

Before we dive into security, it is essential to provide some context about cloud maturity.

Harnessing the full power of the cloud is never an overnight process. It can require years of planning, coordinating, testing, deploying, and optimizing before fully realizing the return on investment. Businesses and managed service providers often rely on cloud maturity models to benchmark performance and track progress.

Cloud maturity must evolve with the scale of your cloud. Concerns, like compute efficiency and price controls, are often the first things companies try to optimize for. But as development pipelines are integrated fully into cloud, end-to-end security becomes a larger concern.

Most cloud maturity models today include security in their frameworks. However, most maturity models don't emphasize them nearly enough - to their detriment.

Security: A Critical Component of Cloud Maturity

Neglecting to account for security can lead to catastrophic consequences. Not only does it open the door to severe data breaches, operational failure, and reputational harm, it can have a devastating impact on your bottom line.

Consider the fact that the average cost of a data breach is now $4.24 million. In the highly regulated healthcare industry, that number more than doubles to $9.23 million. Moreover, in the case of mega data breaches — where bad actors make off with 50 million records or more — the price tag swells to a whopping $401 million.

Personally identifiable information (PII) is the most common type of lost or stolen data in breaches. In fact, 80% of data breaches involve customer PII.

With this in mind, security is now a foundational component of cloud maturity — and something that needs to be top of mind along every step of the cloud migration process.

Despite the precedent of damages and loss of confidence resulting from data breaches and gaps in data governance, many companies are still missing the boat entirely on cloud security.

Cloud Security: A Shared Responsibility

To illustrate cloud security ownership, think of the security "of" the cloud as the responsibility of the provider, and security "in" the cloud as the responsibility of the customer. The cloud providers have gotten better and better at their side of the model, while the challenge has only increased for their customers. There are gray areas and intersections, but imagine your chief concern as the safety of your customers' data, then your internal data and IP, and work backwards from there.

There are three categories for cloud security responsibility:

1. THE CLOUD PROVIDER'S RESPONSIBILITIES

The provider is always responsible for safeguarding the underlying cloud infrastructure. They're also responsible for access, patching, and configuration for the physical hosts and the physical network on which the compute instances run and the storage and other resources reside.

2. THE CUSTOMER'S RESPONSIBILITIES

The customer is always responsible for managing users and their access privileges (e.g., identity and access management), safeguarding cloud accounts from unauthorized access, the encryption and protection of cloud-based data assets, and managing an overall security posture (e.g., compliance).

3. SHARED RESPONSIBILITIES

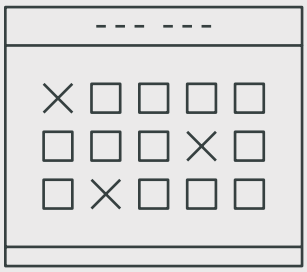
Shared responsibilities typically include infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) functions — like email, AWS / Azure / Google Cloud accounts, messaging, storage, and collaboration platforms.

Start with Benchmarks and Goals

Every cloud security initiative should start with two actions for every cloud environment:

1. DETERMINE A CURRENT MATURITY LEVEL

2. SET A MATURITY GOAL, based on what kind of environment it is, and what data passes through it.



Without reasonable goals and tracking improvement over time, SecOps will be overwhelmed with prioritization issues. Your cloud footprint can grow exponentially, introducing new problems at different scales.

The following guides you through each maturity level telling you what competencies are needed at each level, and what environments you should assign them to.

Cloud Maturity Levels

In an effort to standardize an organization's baseline assessment of cloud security models, we've defined a series of benchmarks as related to a cloud's maturity model.

Maturity Level 0: Exposed

The public cloud is now a large and highly attractive attack surface for bad actors who are actively looking to exploit poorly secured cloud resources and identities. The threat landscape is constantly shifting, and no business or system is safe from intrusion. For example, Microsoft recently warned thousands of cloud computing customers that access keys to their Cosmos DB were accessible publicly via a visualization tool with default access to every database. Since we're talking about Microsoft Azure and it's wide global distribution, it follows that some of the world's largest organizations are potentially at risk.

In our maturity model, Level Zero ("Exposed") means you need to implement basic controls to prevent the most common attacks and public exposures. Best practices around access controls and configurations must be implemented before using your cloud accounts.

The first priority of your maturity journey is to progress all environments to the next level, regardless of environment type or phase in the development pipeline.

At this stage, cloud user roles are often given privileges beyond basic requirements. For example, an admin might grant untrained or unnecessary users permission to modify or delete specific databases. At the application level, improper key configuration and privileges can expose sessions to security risks.

Regulatory compliance complications are common at this level. Even though all leading cloud providers today use well-known accreditation programs — like PCI, NIST, HIPAA, and GDPR — cloud customers are ultimately responsible for keeping workloads and data processes compliant.

The poor visibility at this stage — coupled with the complex dynamics of modern cloud environments — makes it impossible to fully audit individual processes. As a result, businesses at this level tend to have numerous vulnerabilities and misconfigurations.

Add it all up, and data exposure is widespread at Level 0. If you believe your organization is at the Exposed level, take the following steps to get on a better path.

To the right are critical components of a Level 0 Maturity Model.

Secure Your Account

CSPs offer powerful tools for managing and securing accounts. If you want to protect your systems, you need to use them to their full advantage.

For example, in AWS Organizations, you should set up a root user by exception with multi-factor authentication (MFA) and then manually configure account contacts to make sure nothing slips through the cracks.

Separate Workloads and Stages

You may want to consider using multiple accounts to separate workloads and workload stages — such as staging and production.

Using multiple accounts can separate data and resources and use service control policies to implement guardrails. To illustrate, you can use AWS Control Tower in conjunction with Sonrai Security for an easy way to govern multi-account environments.

Use Centralized Identity Control

Identity and access management (IAM) is an essential security requirement in the public cloud. If you aren't using IAM, you're playing with fire.

Centralizing identities using AWS Single Sign-On, Sonrai Security, or other robust authentication tools are necessary. By doing so, you can avoid creating new users or rely on long-term access keys routinely.

Store and Use Secrets Securely

When you can't use temporary credentials (e.g., tokens or one-time passwords), you can control access by storing secrets — like database passwords — in a program such as AWS Secrets Manager, which handles encryption, rotation, and access control.

Maturity Level 1: Basic

Before advancing more sensitive environments to higher levels of security maturity, getting these basic controls applied organization-wide is the priority in your cloud journey.

This maturity level is ideal for use with sandbox environments that don't have any corporate or production assets in circulation. At this level, there's no automation for identity security, data security, or platform security — meaning information is at high risk of exposure.

The following are critical components of a Level 1 Maturity Model:

Basic Multi-factor Authentication

Unfortunately, passwords are largely ineffective as standalone security mechanisms. To enhance your security posture, it is necessary to implement multi-factor authentication (MFA) to reduce threats from brute force attacks and phishing.

Default Security Group Hardening

Carefully examine the cloud provider's default security groups and analyze the associated settings. As a best practice, revoke all rules from default groups to restrict unwarranted inbound and outbound traffic.

Critical Threat and Vulnerability Management

Security teams often focus exclusively on critical threats and vulnerabilities and bypass issues that seem small and insignificant. In a cloud environment, all such issues are of paramount importance and have a potential to impact an organization's operations.

Cybercriminals are well aware of this blind spot and will often flood networks with large volumes of incoming traffic to try and slip past network defenses. That being the case, it's important to expand your security management strategy to account for all incoming threats.

Simply put, strong security schemes require granular protection.

Secure Public Data

Chances are your business has public data that is freely available to a lot of people. Access is one thing — being able to modify it is another.

At this stage, you need to make sure that only authorized individuals can modify something like a spreadsheet. If you make a sheet available to the public, you need to implement access controls to ensure only authorized users can change the data.

Root Account Protection

Whenever you create an account on a platform like AWS, you start with a single identity that contains full access to all AWS resources. This is called the "root" account.

As a general security precaution, never use the root account for everyday administrative or operational tasks. After you set up the account, safeguard the credentials and only use them for service management tasks (e.g., settling your bill).

Light Touch Guardrails

You can further tighten cloud security by setting up guardrails, which are high-level rules for enforcing governance across all accounts.

This includes things like blocking accounts from leaving the organization.

Since this is a security level for an innovation zone, remediation doesn't require complex workflow; resolution should generally involve locking and closing the environment.

Maturity Level 2: Moderate

Maturity Level 2 is generally adequate for non-sensitive workloads in development environments. At this level, security is typically project-based. In other words, there's no consistency or coordination between operations and security teams.

An organization at this level still can't effectively identify and quantify its cloud assets or visualize its cloud environments. Progressing production environments to this stage is your next priority after achieving org-wide Basic Security. After prod has these controls enabled, get staging environments to this level.

The following are critical components of a Level 2 Maturity Model:

Require Encryption

In general, you should have full encryption in place at Level 2 across all data, compute, storage, and database assets. Leading-edge encryption technology protects data while it's in transit and at rest, ensuring that bad actors won't be able to make sense of your data in the event they capture it in the first place. Using TLS Listeners is recommended for secure communication between client and server.

Basic Logging

Logging is the process of recording all event history in a cloud database — which is essential for compliance and governance purposes.

If you're new to logging, AWS CloudTrail is a service that lets you continuously monitor and view changes across your infrastructure. Google Cloud offers a similar tool called Cloud Logging.

Inactive Identity Notification

Inactive accounts can pose a big security risk because they can enable access to sensitive information and systems. For example, someone with administrative access might leave the company or take a hiatus — but their account might still have the ability to enter sensitive areas. If a bad actor gained access to that individual's account, we all know what might happen next.

One way to reduce this type of threat is to use an inactive account monitor. This tool can trigger alerts when accounts become inactive, allowing you to either shut them down or revoke access on an as-needed basis. As a starting point, consider an automated removal of inactive access keys after 90 days.

Privilege Escalation Detection

Methods of privilege escalation have increased significantly, and are harder to track thanks to new serverless capabilities and a larger share of ephemeral compute.

In some cases, this happens naturally. For example, a developer might have their hand in several different projects, requiring entry into multiple databases.

At the same time, privilege escalation can occur when an unauthorized party gains access to a system and uses their credentials to access private information. For example, a hacker could potentially use the iam:CreatePolicyVersion function to create a new IAM policy version and set their own permissions.

This is another area where automation can make a big difference. By automatically tracking user privileges, you can limit permissions and prevent accounts from becoming liabilities — further strengthening your security stance.

Require approvals from inbound ports from the Internet

Monitoring open ports is important, but at Moderate security level, it's recommended to require approvals for certain access. For starters, set up alerts for when remote desktop or SSH access is open to the internet. Monitor open security groups as well, as these are the building blocks of your identity access policy.

It's also important to monitor if ports have large CIDR ranges, as leaving large blocks open needlessly provides paths to breaching a virtual private cloud/network. Sometimes best practices will advise reserving large CIDR blocks to accommodate for growth, so this may become a problem as your cloud footprint expands.

CSPM Basics

Posture Management configurations and compliance checks start becoming necessary at this level. Important "on/off" switches like ensuring MFA is enabled, or making sure that monitoring services like AWS Config are turned on, are the first checks to put in place.

Maturity Level 3: Advanced

Level 3 maturity is the final destination for staging environments (or 'testing,' 'non-prod,' 'UAT,' etc). After all production environments achieve Moderate Security, the priority is to progress environments with sensitive data to this level, then non-sensitive prod environments.

Reaching the Advanced level requires a focus on real world costs. Staging workloads with imminent shipment to prod require a focus on eliminating any compliance issues first. Cross-functional collaboration is key here as governance responsibilities now extend beyond the team building an application.

The following are critical components of a Level 3 Maturity Model:

Tight Governance

At this stage, you'll ideally have a highly advanced identity governance framework in place to manage users and prevent account misuse.

Overprivileged Identity Alerts

By the time an account contains more privileges than required, it could be too late to prevent an attack. The trick is to monitor accounts in real-time with automatic alerts. That way, you can keep close tabs on who's moving in and out of private areas at a given moment.

Self-Escalation Detection

At this point, your team should have the ability to identify over-privileged identities that can self-escalate their permissions. Make sure only authorized admins can enhance permissions.

Trust Relationship Analysis

Trust relationships are links that exist between two domains. They enable access to global groups and user accounts across different domains. That being the case, it's imperative to have direct visibility across all trust relationships to prevent abuse.

Confused Deputy Protection

A confused deputy problem happens when a program tricks a privileged system into misusing its system authority.

You can easily prevent a confused deputy by including the ExternalID condition check in the role's trusted policy.

Advanced Network Security Controls and Change Detection

Strong network security starts with protecting the underlying processes and technologies your team uses to access cloud data.

Ideally, your company will have a combination of tight physical, technical, and administrative security across its network. Achieving this requires close collaboration between IT, security, and network administrators, which we'll learn how to accomplish next.

Temporary Security Credentials

For example: Within AWS, the AWS AssumeRole allows you to establish secure cross-account access. This tool lets you return a set of temporary security credentials for private AWS resources.

Security Tagging

In case you're unfamiliar, a tag is an attribute that contains a key and an optional value. Using attribute-based access controls, it's possible to attach a tag to an AWS resource and grant access to them at scale.

Tags can help organize cloud resources, making them easier to manage and secure. For example, you could use security tags in AWS to flag data and workloads that require advanced confidentiality and compliance.

Credential Hygiene

Most Advanced cloud security frameworks prioritize account hygiene through regularly scheduled maintenance.

This is beneficial, since prioritizing credential cleanup can go a long way in preventing insider attacks. Best practices call for rotating IAM user access keys every 90 days or less.

Maturity Level 4: Resilient

Maturity Level 4 is the goal for production environments without major sensitive data concerns. Continuous runtime analysis comes to the forefront; gaps in monitoring or anomalies must be detected.

Get production environments with sensitive data to this level after getting all prod environments to Level 3. Then you can prioritize staging environments progressing to Level 3.

The following are critical components of a Level 4 Maturity Model:

Least Privilege

Level 4 security requires achieving a state of least privilege, which is the minimum maturity level we recommend setting in any production environment.

If you're new to the term, the principle of least privilege is the concept where users and code have the bare minimum access rights to complete their job.

Enforcing least privilege requires an understanding of any user or compute's true access capabilities beyond the discrete permissions enumerated in their role, group, or IAM record. Once that's understood, then you need the capability to block the various policy combinations or abuse paths that could violate least privilege.

Widespread Automation

At this stage, there's a noticeable shift from manual to automatic security management. By embracing automation, it becomes possible to discover threats and vulnerabilities faster and with greater precision.

As an example, one security process you can automate in AWS is SCAP testing, using AWS Systems Manager and Security Hub.

Advanced Effective Permission Searches

Advanced effective permission searches are a basic necessity for achieving Level 4 security. The goal is to be able to quickly determine what the actual translated permissions are for a user or group on an object.

It's important to be able to rapidly drill down into the effective permissions of an object and view all group membership and inherited permissions that users may accumulate.

DBA Limitations

A sophisticated attacker can gain database administrator (DBA) privileges, enabling them to modify or lift sensitive information from your systems.

As such, it's recommended that you restrict the number of users with DBA privileges to reduce the likelihood this happens. The more users you have with DBA rights, the more at-risk the operation becomes.

Real-Time Alerts

Achieving an advanced level of cloud security is impossible without a robust set of real-time alerts in place.

At this stage, it's a good idea to have alerts in place for monitoring IAM policies, audit tampering, separation of duties, recon, and encryption in transit. In addition, it's worth thinking about using advanced log metric filters to track log metrics and detect unusual patterns.

Version Control

Oversight is necessary to prevent unauthorized users from modifying or updating software — which is why organizations at this level rely on version control systems.

This type of system tracks and documents software changes and can also provide access control when multiple people work on the same system.

Maturity Level 5: Zero-Trust

Simply put, Zero-Trust maturity is the pinnacle of cloud security. Very few companies make it this far. This is the recommended maturity level for all environments with sensitive data.

Once all production environments are at Level 4 and staging at Level 3, you can shift your focus to progressing any sensitive data environments to Zero-Trust standards.

The following are critical components of a Level 5 Maturity Model:

Full Automation

Level 5 leverages full automation, enabling constant awareness and a steady flow of security metrics through systems. This enables organizations to achieve an updated and accurate security baseline at any moment in time.

Customer Encryption Keys

Companies that control sensitive data need to manage their own encryption keys instead of outsourcing the responsibility to a third party. This results in a greater level of control over sensitive information.

Public Base Image Detection

When setting up containers, base images are required as a starting point for creating all other images. Taking images from public repositories can pose a big security threat, as they often are out of date and don't contain patches or updates for known vulnerabilities.

Even the most popular images on DockerHub have many vulnerabilities, and introducing it as a base image can proliferate a vulnerability to all of your subsequent images, or require patching for each one.

As such, it's critical to detect public base images and remove them from production.

File Monitoring

File integrity monitoring is the process of ensuring application files and operating systems are legit by comparing them to a secure baseline. By doing so, organizations can detect and eliminate fraud. The challenge here is 'every change must become a ticket.' Modification, deletion, and creation are all logged and must notify a SOC team.

Deep Auditing

Take a look at any Level 5 cloud deployment, and you'll find deep and continuous auditing — like monitoring login attempts for highly restricted accounts.

It also requires keeping close tabs on management level events and conducting thorough data and management plane traffic separation analysis.

Sensitive File Restrictions

Of course, it's also necessary to restrict sensitive files to prevent them from falling into the wrong hands.

Applying sensitivity labels to privileged content can ensure that only users within your company can open confidential files. With the right tools in place, you can restrict content to certain departments, prevent sharing or forwarding, apply encryption, and more.

Security Maturity is a Journey

Achieving the highest level of cloud security maturity is a journey — not a destination. The most secure companies are constantly assessing their progress and planning for future security needs because they're always evolving.

Far too often, business leaders make the mistake of assuming they have a highly advanced security stance when reality proves otherwise. In large part, this is because most companies today lack the resources monitoring resources necessary to prove their maturity and maintain it.

Yet even when security is a priority, lack of prioritization and contextualization kill the initiative. A SecOps team with a mandate for blanket policy enforcement, without understanding environments or working with Devops, can be just as destructive as they incentivize workarounds and lose credibility. Or if the security team can't keep up with the pace of cloud and doesn't concentrate on the right initiatives, data can be exposed while they're hard at work putting zero trust controls on a sandbox. Either way, "more security" isn't an answer.

The good news: by partnering with a leading cloud security provider, like Sonrai, you can fortify your security posture and understand what environments and policies to prioritize giving you the resources and expertise you need to protect your crown jewel data.

Learn More

With Sonrai Dig, you gain access to continuous platform, identity, and data security. Dig runs on a sophisticated graph database that identifies and monitors all relationships between data and identities across multiple cloud environments in real time.

Sonrai can also help operationalize your security strategy by pointing out specific areas you need to address. The Sonrai team will show exactly where problems exist — and the specific steps you can take to advance to a more mature level of security.

By partnering with Sonrai, your company can ultimately save time and money while fortifying your networks and putting yourself in a position to ward off attackers for years to come.

Request a Demo Today

sonraísecurity.com
info@sonraísecurity.com
646.389.2262