AllCloud

The Best Practices for Cloud Security Operations on AWS

CONTENTS

Cloud Security Baseline

The responsibility for the security of your organization's data and applications on the cloud is your own to govern. This might sound like a lot to manage, but with the right tools and support, this shouldn't stop you from embracing the many benefits of cloud infrastructure on AWS. Here's our baseline, detailing which pillars you need to focus on in order to implement early and continuous cloud security. We've highlighted some of the necessary best practices for overcoming challenges and staying in control of your security posture. Following a security baseline will make all the difference.

Identity and Access Management

Who can access your information on the cloud, and who is authorized to take action? When you're dealing with complex organizations with hundreds or thousands of employees, projects and workloads, you need visibility and control over roles and policy creation. This isn't just a 'nice to have' for optimization and visualization, it's often a 'must-have' for compliance and security.

Setting up and defining your IAM playbook is foundational for strong security on the cloud, and can be a precursor for automation opportunities that will streamline security overall. This could be anything from detecting anomalies or updating security controls, to patch management or the deployment of changes to security codes.

Logging and Monitoring

Many companies move to the cloud for improved agility, performance and scalability. Without the right approach to logging and monitoring, you won't be able to fully realize these benefits, and you'll probably experience a negative effect on how you handle incidents or keep on top of security concerns overall.

Setting up monitoring should be one of the first items on your do-to list, including visibility into system and performance changes, operational health, and how to stay on top of the resources you're using, especially if you're paying for only what you use.

You should find the right tools, starting with cloud-native services like AWS CloudTrail and AWS GuardDuty and complement with 3rd party solutions as needed in order to set **alerts for the metrics that you want to watch in granular detail, integrating these with your SIEM and forwarding events and logs to the right place, alongside actionable insights** for escalation and action.

Infrastructure Security for AWS

It's important to think about the network access that you want built into your AWS infrastructure. Creating a security playbook will help you define exactly what you need, controlling the private networks and connections you want to allow for your organization.

The security playbook should define a strategy for Amazon VPCs (Virtual Private Cloud) and subnets as well as establish a baseline for security groups. In the Playbook, **VPC Flow Logs should be enabled and configured to deliver logs to a designated logging tool.** This goes for monitoring too, where monitoring rules should be designated and implemented. Other strategies that should be addressed in the playbook are Direct Connect/VPN for connections with on-premise environments and CIDR strategy for better governance over IP addressing within your organization.

There are two important DevOps practices that should be leveraged. First, **building the baseline security rules with infrastructure as code**, so that your best practices are automated and built-in to protect you from vulnerability. Second, **developing AMI bakery with the SSM and Inspector agents installed to speed up the boot time of your EC2 instances.**

When set up correctly, AWS can also ensure that you have encryption across all services, even when traffic is in transit.

Data Protection on the Cloud

For most businesses, losing control over their data would put their customer trust in jeopardy, and risk disclosing sensitive information. Data protection is, therefore, a top priority for many companies moving to the cloud. **Ensuring that your data is always encrypted both in transit and at rest is integral,** and businesses need to understand how to **manage the AWS Key Management Service (KMS) to access and protect data and storage in a secure, compliant and yet accessible way.**

When it comes to data storage, you have many secure options depending on what you're looking for in terms of cost, performance and capacity needs. For some businesses, the default S3 encryption is the right way to go, while for use cases like data warehousing or analytics engines, Elastic Block Store (EBS) may be a smarter choice.

Incident Response

Preventative measures will only do so much. Today's threat landscape is marked by the unknown; zero-day threats, and new attack vectors that cannot always be predicted in time. However, limiting dwell time will make the difference between a manageable incident and something your business cannot recover from. **Define a cloud-specific incident response playbook that includes a suitable ticketing management system and the right investigative tools, automating IoC detection and response at a code level.** The results will be clear. You will be able to quickly find, isolate and remove any threat to your cloud infrastructure.

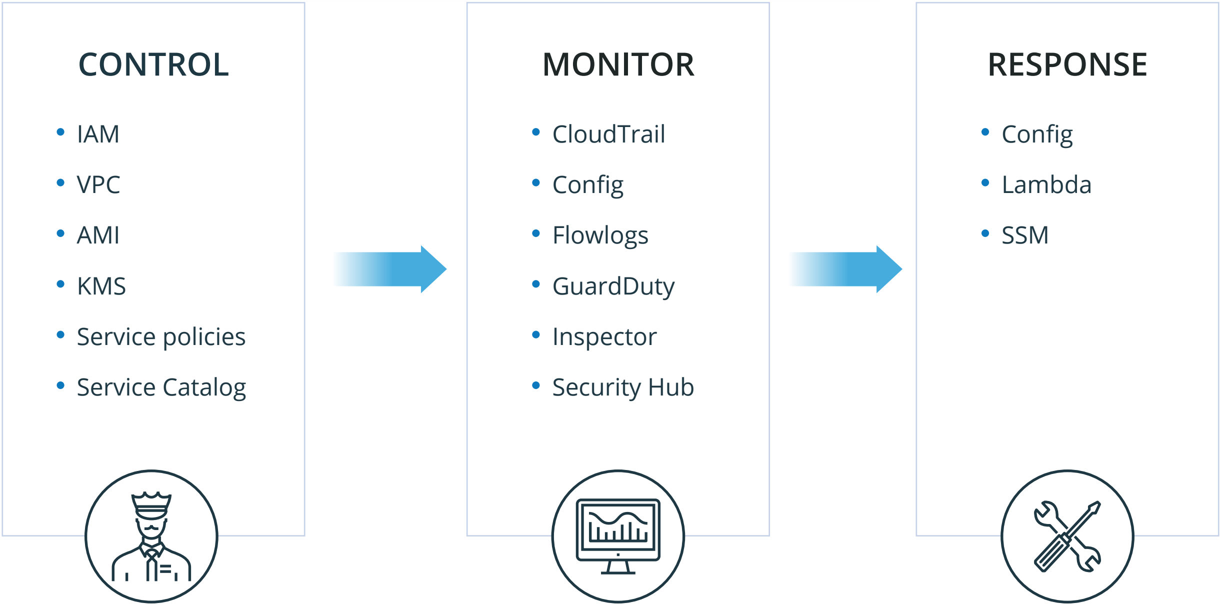
According to the latest SANS report, 50% of companies have a lack of access to the system information and log files that are needed for forensic examination of a security breach, while 40% have difficulties because of multi-tenancy. Creating a playbook for incident response means that your company does not suffer from lack of visibility, event data, evidence, skills gaps, or missing controls and processes when you're trying to act quickly in crisis mode.

Cost Governance and Control for Enterprise IT

Of course, your security procedure needs to be affordable, or you don't have a viable cloud business at all. The right process starts with setting up cost centers and account aggregation, with budget management and a cost allocation framework considered from the very start. This lends transparency to the whole project, and provides a baseline to use for both budgeting and decision making if and when things change during the business transformation process.

If your instances start costing more than your expectations, alerts, automated actions and procedures can streamline your digital workflow. As well as tracking spending and costs, this process integrates FinOps alongside your overall cloud strategy. This ensures you avoid the irresponsible financial management that has a negative impact on 80% of financial and IT leaders when moving to the cloud.

AWS Security Lifecycle



CONTROL

- IAM
- VPC
- AMI
- KMS
- Service policies
- Service Catalog

MONITOR

- CloudTrail
- Config
- Flowlogs
- GuardDuty
- Inspector
- Security Hub

RESPONSE

- Config
- Lambda
- SSM

Bringing it all Together for a Secure Move to the Cloud on AWS

With the right advice, and a strong 'best practice' playbook to follow, moving to the cloud doesn't have to open the door to security issues and lack of control. In fact, the tools are out there to improve and enable security at the same time as embracing the scalability, flexibility, and innovation of a cloud infrastructure.

If you're looking for a secure way to move your workloads to the cloud, with these best practices included as standard, AllCloud has over 11 years of experience managing hundreds of cloud deployments. Check out our white paper on our Enterprise Landing Zone solution, an automated framework to help your organization go from 'nothing' to 'running' on the cloud.

A strong cloud requires proven best practices, advanced technologies, and a trusted advisor. Consult with an AWS security expert today!