StackZone

SOC 2

Blueprint

In this document, you will learn how to improve your AWS cloud infrastructure by aligning your systems to SOC2 standard cloud requirements using StackZone'sCloud Management Platform. This results in a secure, monitored, resilient and SOC 2 compliant cloud environment because the goal of StackZone is to make it easy for businesses to run their workloads so they can focus on selling their products.

Healthcare industry Blueprint with StackZone's Cloud Management Platform. This blueprint was designed based on industry best practices as well as our customers' feedback. **StackZone was built with our customer's feedback in mind. Our mission is to make it easy for businesses to manage their AWS cloud, so they can focus on running their business.**

Implementing the SOC 2 blueprint enables you to take your AWS workload to the next level, putting special focus on **security, compliance, reliability, and cost optimization.**

StackZone's SOC 2 setup includes the necessary components to support and build compliance according to SOC 2 cloud requirements. This ensures that every organization has all the cloud-related tools needed to achieve the certification.

For the core accounts **(Shared Services, Log-Archive and Management)**, we build a default-compliant Amazon virtual private cloud (VPC), an Amazon S3 bucket with a lifecycle policy to store logs for up to 7 years, and we delegate some security service administration to the security account.

We also enable the following services on the **security account:**

A global centralized Amazon GuardDuty, GuardDuty Remediation (NACL Retention (720 h) and Macie aggregation for all accounts within your StackZone organization. That gives your SecOps team full visibility into your findings. Any new account gets invited to the centralized Amazon GuardDuty Detector and Amazon Macie.

Once StackZone has been deployed, we build a number of **Service Control Policies (SCPs)** for you to apply to the accounts. These Guardrails allow you to deploy your workload in compliance with SOC2 cloud recomendations.

These functions help you simply manage and monitor your organization, but what about the accounts and environments where you will be running your workload?

On every account and region, we deploy the following **Baseline Services:**

CloudTrail Multi-Region

Allows you to track every change made to your AWS infrastructure and activity on it.

CloudWatch Alarms

Remain up-to-date and get notifications on every change or threat to your workload with StackZone CloudWatch alarms.

AWS Config Rules, and Aws Config Global and Local Aggregators

We deploy 82 AWS Config Rules. AWS Config rules ensure you actively monitor your resource configuration, which translates into continuous monitoring of the security and compliance of your resources. In addition to this, more than 51 auto-remediation rules can be easily implemented. The auto-remediation rules ensure deviations are automatically solved.

Enable AWS Budgets in all Accounts

AWS Budgets allow AWS customers to set custom budgets and monitor their costs and usage over a set period of time. Once you have chosen your desired thresholds, StackZone is then able to set up SNS notifications and email notifications, so that you are informed when actual or forecasted costs and usage exceed your set amount.

Enable AWS Backup and restore

Ensure your EC2 Instances, EBS volumes and RDS instances are protected by including them in a backup plan by just tagging your resources.

AWS SSM Associations

StackZone enables a variety of AWS SSM Associations. Update SSM agent will try and update the AWS SSM agent installed on your SSM managed EC2 instance. QueryScanPatches will gather information around software patches and GatherInventory will gather information about your EC2 instance so you can see it from the SSM dashboard in the AWS console.

Amazon EC2 Isolation

In case an EC2 instance is compromised, or you need to remove internet access while you troubleshoot a serious issue; Amazon EC2 Isolation allows you to isolate an EC2 instance by just adding a specific tag.

So far, we've covered the most important and general services and tools **StackZone** provides our customers when applying the **SOC2 Blueprint.**

As always, this is just the first step because, as part of the **StackZone** community, you will receive continuous updates that will allow you to permanently improve your AWS cloud workload. We do so based on best practices, standard updates, and our customers' feedback. **This means you will be able to request the features you need, and our commitment is to evaluate them and add them to our roadmap.**

Would you like more detail on everything that's deployed via this Blueprint, to see if this is the right blueprint for you to adopt? Access to https://help.stackzone.com/article/stackzone-aws-soc2 or simply book a call with us and take your AWS workloads to the next level.