CHECKLIST

Checklist for Ensuring Security and Compliance in the Cloud

The cloud has provided a means for organizations to accelerate their digital transformation, to scale and innovate at speed. However, the fast-paced and dynamic nature of the cloud has introduced new security and compliance challenges. There are too many resources, interfaces, and policies to track and govern.

Below is a checklist of items that companies should take into consideration as they migrate to the cloud:

Security and Access Policies Validation

Not having adequate restrictions or safeguards in place to prevent unauthorized access and account hijacking can put your organization at risk. If your business manages sensitive data, access to the system and its data needs to be restricted. This means allowing only authorized users to make defined changes.

Be sure to implement security measures that include minimum password complexity, prohibiting password reuse for a certain number of generations, and disabling password after an inactivity period. Also review permission controls to ensure that authorized users are given only the necessary permission to perform their jobs. Giving widespread access can open your organization to risks.

The access and security policies need to be continuously reviewed and validated to ensure compliance.

CHECKLIST

- ☑ Security and Access Policies Validation
- ☑ Compliance Standards Assurance
- ☑ Misconfiguration Remediation
- ☑ Audit Reporting
- ☑ Inventory Discovery

Compliance Standards Assurance

Today's companies are subjected to a number of internal and regulatory compliance requirements. Each year there are new regulations to follow and old regulations that still require compliance. Mapping your infrastructure configurations to compliance frameworks including GDPR, HIPAA, NIST and CIS can be challenging.

Some solutions can provide a list of predefined validations to run against your cloud infrastructure to assess whether controls are properly enforced. If there are policy violations, those will need to be corrected as soon as possible. Some solutions will automatically revert policy violations back to a known compliant state to ensure that your infrastructure is adhering to the compliance policies without requiring human intervention.

Misconfiguration Remediation

Configuration drift remains one of the most common security concerns for organizations moving to the cloud. Cloud misconfiguration can be easily exploited to gain access to your data, thus exposing your organization unforeseen risks. It is not uncommon to take hours or days to correct misconfiguration. In a recent survey, 86% of respondents indicated that their mean time to remediation is often one day. The longer it takes to find and correct a misconfiguration, the higher the risk of a massive security breach.

Select a security solution that offers automated remediation of misconfiguration. With automated remediation, unauthorized changes are reverted back to a previously known good baseline as soon as they are discovered. This ensures that your infrastructure is always in compliance.

Audit Reporting

The audit process can be time consuming and resource intensive. Auditors want proof of compliance or risk severe fines. Detailed logs are necessary to show evidence of compliance to auditors. The logs should include the type of change, when it occurred, where in the infrastructure environment, what specific resource and who made the change.

If you are using a security solution that offers library of compliance controls, these can serve as proof of compliance. Companies can easily show that they are enforcing and maintaining compliance for a particular standard.

Inventory Discovery

After you've migrated to the cloud, your inventory is constantly at risk of changing without your knowledge because it is so easy to create and destroy resources in the cloud. You need a way to continuously scan your environment to automatically track what is actually there.

Performing an audit scan of all your cloud resources can provide you with an accurate inventory of what is in your cloud environment. And only then, can you determine which cloud assets are compliant and which ones are non-compliant.

Conclusion

As companies migrate to the cloud to leverage its benefits, security and compliance must be an integral part of the migration. Selecting the right security solution can go a long way to help alleviate some of the stress and risks associated with migrating to the cloud.

Fugue's automated platform built on policy-as-code, continuous monitoring and automated remediation helps to secure your cloud infrastructure and ensure that it is always in compliance.

To learn more about Fugue and how we can help eliminate cloud risks, visit www.fugue.co.

About Fugue

Fugue, a leader in cloud infrastructure automation and security, provides solutions to ensure that enterprise and public agencies cloud resources are always provisioned according to a single source of truth—and stay that way throughout the resources' lifetime. Fugue is privately held and headquartered in Maryland. Fugue was names a Cool Vendor in Cloud Computing 2017 by Gartner.

aws partner network
Advanced Technology Partner