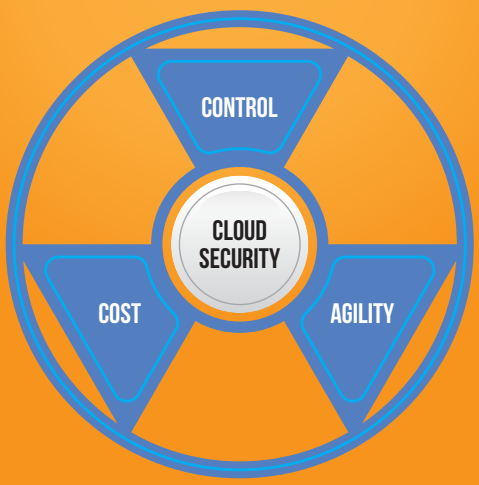
MontyCloud

Autonomous cloud security and compliance management – the foundation of a secure cloud

The pandemic has accelerated digital transformations unlike any single event in history. While cloud enables application developers with amazing possibilities and modern development tools, it is also a challenge for infrastructure administrators and CIOs. For IT teams, cloud security is a constant balancing act between control, cost, and agility. In this paper I discuss five easy steps you can take today to balance your security and compliance profile alongside costs and agility.



1 833 329 2677
sales@montycloud.com

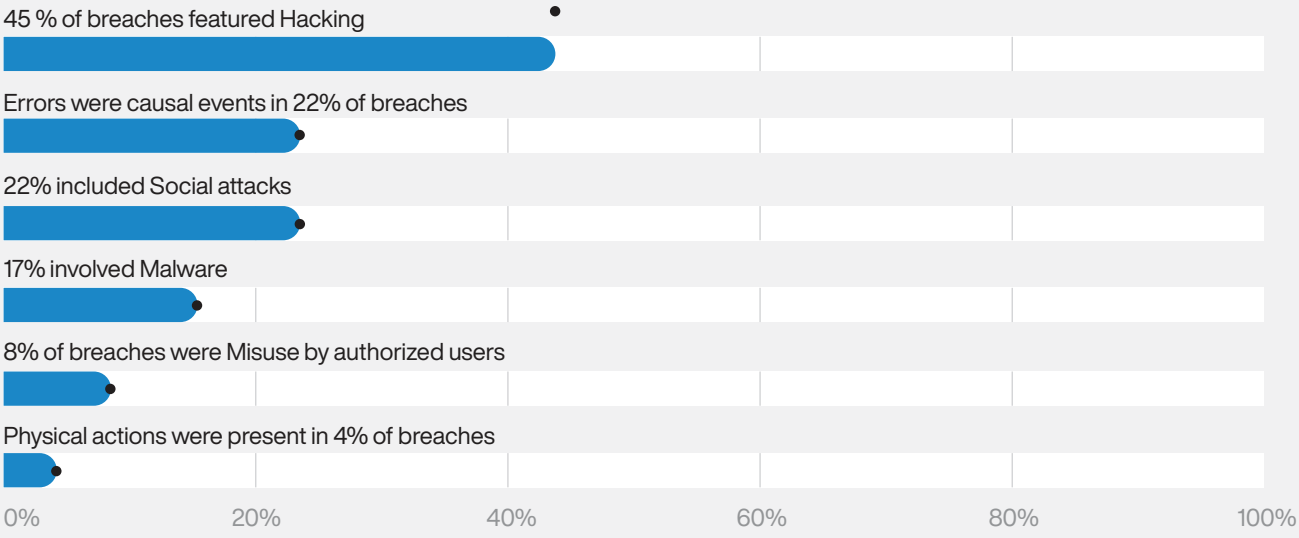
aws partner network
Advanced Technology Partner
Cloud Management Tools Competency
Public Sector Partner

Insufficient expertise is the top challenge for IT security teams

Cloud vendors such as Amazon Web Services have done a great job at addressing many of the cloud challenges. AWS has 27 services ranging from AWS Identity and Access Management (IAM) to AWS Security hub. Each of these 27 services come with their own configuration settings and APIs. For large organizations with cloud infrastructure developers, this is a blessing. But most IT teams that own digital transformations do not have the skills to effectively use these rich API surfaces. An IDC survey found that 66% of the respondents stated that insufficient personnel and expertise is their top concern to managing cloud security.

Verizon's 2020 Data Breach Investigations Report revealed that 20% of the 3,950 high profile breaches reported in 2020 were a result of misconfigurations and errors (image 2), second only to organized hacking.

Top reasons for security breaches



Source: Verizon 2020 Data Breach Investigation Report

Cloud services when implemented properly are transformative. IT teams can overcome their challenges through by

1. Spending time on upfront planning
2. Automating frequent assessments of their security and compliance posture
3. Implementing policy based remediations.

In this paper, I discuss five easy steps you can take today to balance your security and compliance profile alongside costs and agility.

1 833 329 2677
sales@montycloud.com

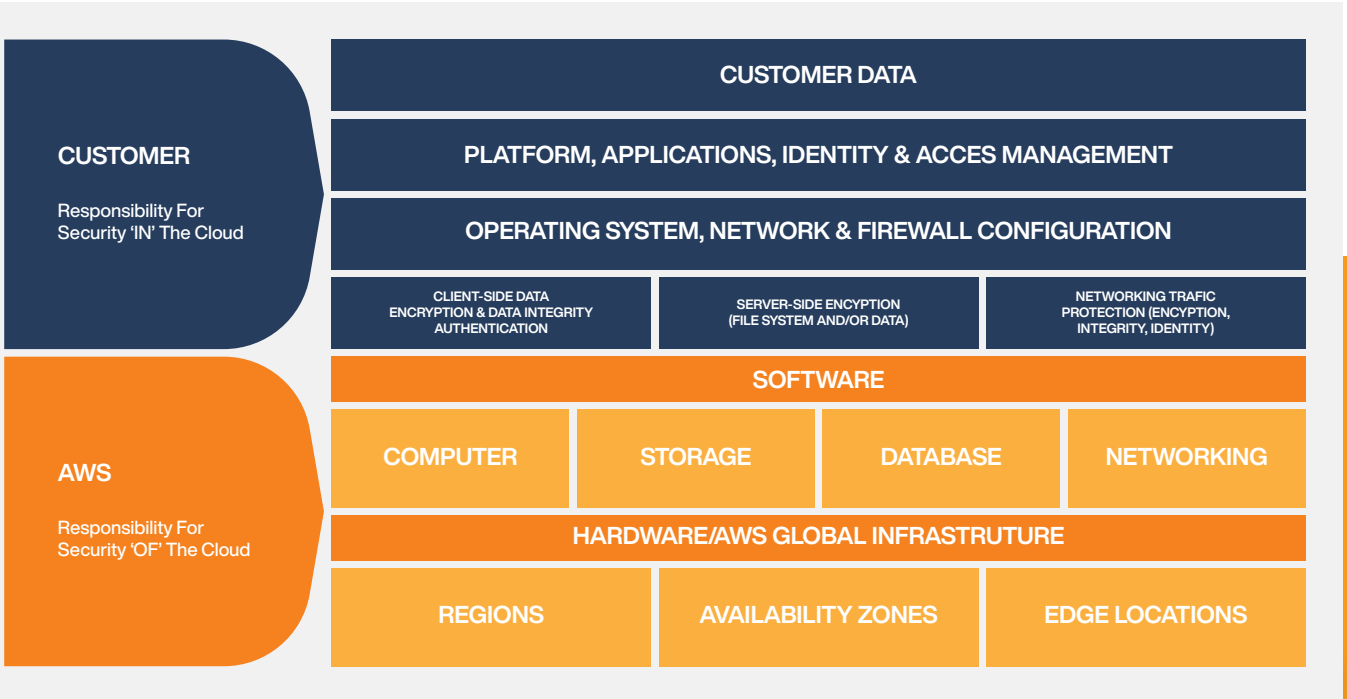
1 Understand your responsibilities in the shared security model.

Over the past decade all major cloud vendors have invested significantly in cloud security. Their underlying infrastructure that powers your applications is very secure.

It is common for customers to assume that once they move to the cloud, security and compliance is the responsibility of the cloud provider. In reality, security and compliance in the cloud is a shared responsibility between the customer and the cloud provider. Your cloud provider does not know which applications are running in your account and does not have access to your data. This makes it impossible for your cloud vendor to secure and enforce compliance on what they don't know.

All cloud vendors including Amazon Web Services operate under the shared responsibility model. This means your cloud provider has the responsibility to secure the underlying service, the host operating systems, the physical hardware, and the datacenters including regions, availability zones and edge locations.

You, as the customer, have the responsibility to protect your application stack, which includes your guest operating system, and all the application components such as your database instance, underlying storage user access controls, network traffic to and from your application. AWS have this useful image on their website, which explains the delineation of responsibilities well. (image 4 – and source it please). Understanding your responsibilities is the first step to designing a robust security posture. This understanding will help you find the tools to continuously detect and enforce security and compliance policies.



Source: AWS Shared Responsibility model

2 Know what is running in your environment.

Knowing what is running in your environment is the next step towards robust cloud security. A survey of 300 CISOs conducted by research firm IDC ranked lack of adequate visibility into cloud resources as one of the top 3 reasons for cloud security breaches. The other two being misconfigurations and identity & access management errors.

The power of a well-managed cloud infrastructure is that you can enable your users to provision resources and scale up or scale down on demand. This means new cloud resources are coming live or going offline all the time.

For example, it is not uncommon for your development organization to spin up a dev/test environment and forget to take it down at the end of their task. Sometimes these can just be a group of compute instances such as Amazon EC2. Unless automatically enforced, these environments rarely comply with your organization's security and compliance standards. Untagged, abandoned or orphaned resources can go rogue very quickly. The recent Solarwinds breach is a prime example. The perpetrators penetrated through a dev-test system and introduced malicious code into production systems.

Getting continuous visibility into your cloud resources, keeping a real time inventory of what resources are running along with which application and/or user owns a resource is therefore vital.

Your CloudOps platform should help you discover, tag, classify and verify every resource against your security posture. It should automatically remediate and trigger an alert every time a new resource comes online or goes offline. It should also immediately detect and take action against untagged, abandoned or orphaned resources.

3 Get an assessment of your compliance and security posture at least once a day.

Compliance and security posture assessments provide a status check on your systems and applications relative to your security policies. A good place to start is with the standards for your industry and the best practices defined by your cloud provider. Amazon Web Services has documented about 200 these foundational security best practices that surface through AWS Security Hub and 56+ conformance packs. They cover commonly used industry standards such as NIST 800 171, NYDFS 23, PCI DSS 3.2.1, CMMC, CIS, FedRamp and HIPAA that are available through AWS Config. You can download the control list and manually run your assessment checks periodically. Another alternative is use tools like MontyCloud DAY2™ that use the AWS defined best practices as the baseline and enable you upload your own policies. You can also configure tools like DAY2™ to run assessment checks at predetermined intervals and give you an assessment of your security and compliance posture.

4 Define policies and automate remediations.

Central public cloud strategies will always lag public cloud usage. "Unapproved" cloud consumption is the new reality. IT teams that make successful digital transformations, embrace the controlled chaos. The most efficient path for central IT teams is to define robust security and compliance policies and to implement tools and systems to continuously check and automatically remediate drifts or respond to alerts.
Industry experts agree that there are generally three levels of policies –

1. Organizational policies, that you can implement at the account level, so they are inherited by all authorized users and resources.
2. Resource level policies, that define resource specific controls. For example, you can define a policy where all S3 buckets provisioned within an account or by a user group such as Dev/Engineering are locked by default.
3. Issue specific policies, where you define remediations for specific scenarios such as when you discover an orphaned VM. Your first step is to check if it is tagged and associate it with the right user/application. Then you may check which user/application provisioned it and finally if you cannot determine the owner raise a flag and shut the VM down.

Your cloud providers such as AWS, your industry bodies and even open-source channels maintained by security experts such as ElectricEye provide a good baseline but you must define and implement your own policies, controls and remediations that suit your organization. You can then leverage tools like MontyCloud DAY2™ to automate checks and remediations.

1 833 329 2677
sales@montycloud.com

5 Get an assessment of your compliance and security posture at least once a day.

Last but not the least keep an audit trail. Implement tools that give you operational dashboards and an assessment report at least once a day. In addition to alerts, you should also get actionable recommendations.

Cloud environments are dynamic. There is room for a lot of noise in your dashboards and alerting systems. Automating remediations can go a long way. Equally important is to identify non-issues and suppress them.

Finally, ensure that you maintain an audit trail of all events that trigger specific actions and of the actions themselves. Audit trails help you analyze usage and access patterns. Frequent analysis helps you iterate your security policies and compliance standards and remain responsive to your business.

MontyCloud DAY2™ helps you Visualize, Analyze and Automate.

MontyCloud DAY2™ can automate free security and compliance posture assessments in just five easy steps. Signup for a free MontyCloud DAY2™ account today and immediately:

1. Assess your cloud against 200+ AWS security best practices and 164 compliance checks across 60+ industry specific standards and 72 AWS services.
2. Get continuous visibility of all your cloud resources and services across cloud accounts and regions.
3. Instantly get an inventory of all resources across cloud accounts and regions.
4. Group and manage your cloud resources in their applications or departments context.
5. Identify abandoned, and unused resources and act such as reclaim the resource or isolate the resource for further investigation.

1 833 329 2677
sales@montycloud.com