Payatu

Cloud Security Assessment Datasheet

OVERVIEW OF THE SERVICE

As more and more organizations undergo digital transformation, the adoption and integration of cloud-based tools and services increases. The migration to the cloud has also led to an evolution of distinct cybersecurity-related concerns for these organizations. For modern-day enterprises it is important to secure their cloud applications and infrastructure, and the first step towards it is – cloud security assessment.

Payatu's cloud security assessments are known for delivering actionable insights that help clients in accelerating the process of securing their cloud servers. Its layered security review has proven to be extremely beneficial for the client in building scalable and secure applications. This service-provider's cloud security assessment enables clients to identify potential vulnerabilities in their cloud environment, exponentially.

KEY ATTRIBUTES

Payatu's objective is to perform controlled attack, conduct a configuration review, security tooling, penetration activities, and security assessment to evaluate the overall level of security of the cloud and what sets Payatu apart is

A combination of realistic and abstract approach

Having substantial experience in this arena paired with learning the cloud environment conceptually helps the Payatu Bandits to define a process and roadmap specific to the client.

End-to-end defining of the scope

It is important for Payatu to address all types of potential attacks on the client's cloud infrastructure, which is why its scope covers cloud asset discovery, cloud configuration review, access control, authentication review, internal assessment and external assessment.

Ultramodern tech integrations

Payatu strives to widen the attack surface to ensure identification of all vulnerabilities, and it does so by integrating different internal, external, and modern third-party tools and software.

Reports that go beyond reporting

Generalized reporting is a drawback that can make any cloud security assessment futile. With Payatu, clients get a detailed report of the test cases that worked, a granular breakdown of the vulnerabilities, failed test cases, mitigation strategies, and recommendations.

The Payatu Extra Mile

Payatu goes an extra mile to retest and revalidate the gaps and security misconfiguration, offer guidance to the in-house security team of the client on the mitigation plan, get the compliance of the cloud infrastructure with the mandated standards, and a lot more.

Payatu

KEY BENEFITS

The ultimate goal of Payatu's cloud security assessment is to unravel the real picture of the threats to the clients' cloud environment and help them in mitigating all the misconfigurations.

01 Protection against Potential attack

Identifying security gaps can help clients protect themselves against attacks and vulnerabilities such as SSRF attacks, data loss, unauthorized data access, DoS attacks, bot attacks, etc.

02 Data Integrity is Ensured by Checking Encryption

To ensure that the clients have complete control over the integrity of their data, encryption checks are performed. The encryption check will look for weak/no encryption being used by applications/services to encrypt customer data/metadata and store or use the same for its own purpose.

03 Reduced Risk with Access Control Check

In order to help the client with reducing several risks such as insider threat and sabotage, data loss/leakage, and compliance violations, cloud environment is tested for poor access control to cloud resources. In this test, Payatu looks for different levels of user privileges escalations which includes Attribute-Based Access Control (ABAC).

04 Identification of Information Leakage to Protect Brand Reputation

Data breaches are the most common incidents that can damage corporate reputation. Payatu makes sure to check for any kind of information leakage happening in normal as well as abnormal communication inside and outside cloud infrastructure.

05 Granular Understanding via Extensive Documentation

In the documentation, the details of the test cases, scan results, vulnerabilities found, and proof of vulnerabilities are captured along with an overview of the current security state of the target and how the customer can improve it.

06 Build Brand Confidence for Users

Clients can make security their value proposition in the competitive digital market by establishing trust within their users/clients by offering security as their brands' proposition.

07 High-Quality Testing

9 out of 10 industry leaders have made it a point to recommend Payatu's services to other pioneers because of the experiences they had while getting their cloud infrastructure tested. This has been made possible because of the best-in-class hires who have proved their mettle by going beyond their scope of work, even before they're hired.

Top Customers

NXP TATA DIGITAL SSMC

MEDLY navi

ENGAGEMENT MODELS

You choose what works best for you!

Payatu offers different engagement models to let the client decide what floats their boat when they avail themselves of the cloud security assessment service. They can choose from

01

Time-boxed Approach,

where the client shares the details of the scope of assessment with Payatu and the service provider evaluates the time and investment required to execute the project. This evaluation is done with the help of complexity models

	Low Complexity	Medium Complexity	High Complexity
Compute (EC2,VMs)	20-30	30-80	80-120
Storage (S3,Containers, Blobs)	30-40	40-50	50-80
IAM Roles, Policies	10-20	20-30	30-40
Database (RDS, Azure DB)	5-10	20-30	30-40
Functions, Lambda	10-20	20-30	30-40
Other Services	10-20	30-40	40-50
Penetration Testing + Config Review			
Initial Testing (#of Mandays)	12	16	20
Retesting (#of Mandays)	2	3	4

Note

- It is considered that number of subscription and account is 1.
- Anything beyond the above table will be considered as custom effort.
- This model can be used for 2 subscriptions with total count of resources not exceeding the range mentioned above.

02

Staff Augmentation,

where the client leverages the skillset of Payatu's security consultants and has them work with their in-house security team for an agreed-upon period of time.

03 Master Services Agreement

Minimum duration & projects commitment,

where Payatu conducts a T-shirt sizing of the client-proposed minimum scope and classifies each project as per complexity.

Minimum T&M effort commitment,

where Payatu proposes investment mapped with resource skill, resource experience, duration of T&M engagement, based on the client-proposed minimum commitment.