threat stack | powered by amazon web services

Top 10 Best Practices for AWS Security

threat stack | powered by amazon web services

TABLE OF CONTENTS

threat stack | powered by amazon web services

INTRODUCTION

Security on the AWS Cloud is not comprised of one perfect solution for everyone. Every organization has unique security challenges and business goals. This means that you need to tailor a security initiative to suit your organization's needs.

This eBook will explore what is involved in creating a comprehensive security posture on the cloud, best practices for AWS security, what AWS' role is in your security stack, and how Threat Stack can help you figure it all out.

threat stack | powered by amazon web services

THE STATE OF AWS SECURITY

Market Trends

Combining DevOps and Security

With the rise of DevOps and shift of responsibilities to these roles, finding a way to merge your development, operations, and security initiatives is becoming more important than ever. DevOps can help integrate security earlier in the development process, ensuring built-in security practices and infrastructure.

Trust but Verify

In the days of continuous delivery, more people have access to production and more systems are interconnected to streamline operations. So the question comes up—how do you verify whether or not activity is legitimate? Organizations want to be able to give their developers access to production to build faster, but there must be visibility into the activity occurring there.

Visibility into your workloads helps expose risky anomalies.

Sharing the Load

As you'll see throughout this eBook, visibility and rapid detection are some of the most important parts of a comprehensive cloud security posture. Organizations are starting to take security beyond their security teams, to their entire workforce. By implementing the right tools and processes, the entire organization is empowered and responsible for keeping your cloud environment safe.

Cloud Security Needs

While there is no one-size-fits-all security solution, there are critical elements that must be addressed to achieve confidence in the security of your deployment. Firewall and network segmentation needs to be managed, IAM policies applied, and visibility into your workloads need to be gained. Security risk detection must start at the workload and infrastructure levels. Establishing behavioral baselines for both users and software allows organizations to identify policy violations, anomalous behavior, malicious activity, remote code exploit, and data loss.

threat stack | powered by amazon web services

THE STATE OF AWS SECURITY

Common Security Challenges

Cloud security is at the top of every organization's mind before, during, and after their migration to Amazon Web Services. The following are a handful of common cloud security challenges:

Overcoming a lack of visibility
You're running more applications on the cloud than ever. You have more people accessing those applications every day. Files change on a per-second basis. Without a security strategy in place to keep track of this near-constant activity, it can be difficult to pick out what activity is malicious or suspicious.

Prioritizing a security strategy ahead of controls and tools
You must decide early on whether to implement a security strategy first or controls and tools. In most cases, having a strategy in place first will lead to smoother, more effective security from day one.

Improving confidence in a cloud provider security
Security on the cloud is becoming a discussion earlier in the cloud migration process. You have pertinent questions to ask AWS and your cloud security provider about compliance, accessing log data, dealing with incident response, and more.

Establishing who is accountable
In the event that a security incident does occur in your cloud environment, you want to know who is liable and what the appropriate actions are. AWS' Shared Responsibility Model sheds light on this subject.

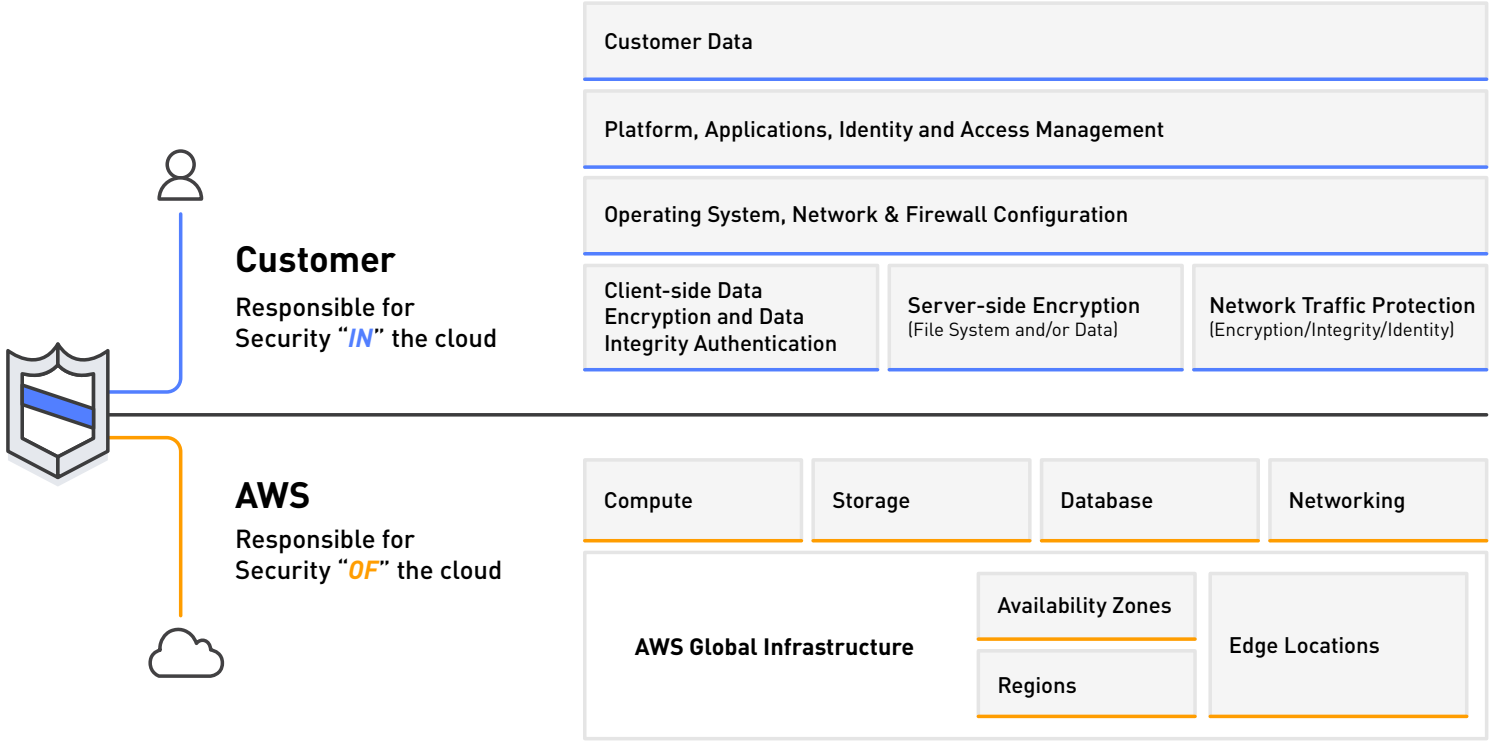
Understanding the lure behind cloud security attacks
When you operate in the cloud, you're likely trusting a lot of sensitive data to your cloud provider. This makes it a great target for attacks. More often than not, security incidents occur because of credential threat, not sophisticated zero-day attack against cloud providers themselves.

threat stack | powered by amazon web services

SHARED RESPONSIBILITY MODEL

When evaluating the security of a cloud solution, it is important to understand and distinguish between:

- "Security of the cloud" — Security measures that the cloud service provider (AWS) implements and operates
- "Security in the cloud" — Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services



threat stack | powered by amazon web services

SHARED RESPONSIBILITY MODEL

amazon web services

What Part Does AWS Play?

AWS ensures the security of the AWS Global Infrastructure of 42 Availability Zones within 16 geographic Regions around the world, in addition to compute, storage, database, and networking capabilities. AWS is also responsible for the security configuration of their managed services including Amazon DynamoDB, Amazon Elastic MapReduce, and more.

What Part Do You Play?

You retain control and ownership over your data and what security you choose to implement to protect your own data, platform, applications, systems and networks, no differently than you would for applications in an on-site data center. This control over security implementations allows you to decide what security measures are necessary for your industry and organization, specifically.

threat stack

How Does Threat Stack Help?

Being able to see everything that is happening within your cloud environment is the only way to ensure you are keeping it secure. Threat Stack provides host-level visibility and detection that tells you immediately when there is anomalous behavior that could indicate potential external attacks, insider threats, and data loss.

threat stack | powered by amazon web services

TOP 10 BEST PRACTICES FOR AWS SECURITY

There are many actions to be taken to ensure your AWS environment is secure.
Get started with this Top 10 checklist:

1 **Leverage multi-factor authentication**
Using a standard username and password combo as the sole gatekeeper between your data and hackers is no longer the safest bet. Securing access to your cloud applications with multi-factor authentication adds an additional safeguard against wrongful access. MFA requires users to take an extra step like receiving an access code on their phone or onetime passwords to complete the login process so that even if a hacker obtains login credentials, they aren't able to log in.

2 **Utilize identity and access management**
Users expect to access your applications fast and with as few roadblocks as possible. As an organization, you must find the balance between streamlined access and secure data. Identity and access management (IAM) combines the three elements you need to achieve this: identification, authentication, and authorization.

3 **Maintain strong visibility into your cloud environment**
Blind spots are the enemy to any security posture. Having deep visibility into your cloud environment at all times is essential to maintaining operations, pinpointing issues, and adhering to compliance standards.

4 **Implement end-to-end encryption**
Cloud security should be more proactive than reactive. Encrypting data end-to-end is a proactive move that ensures that even if the worst happens—your data gets into the wrong hands—it'll still be secure and unreadable.

5 **Monitor file integrity**
Establishing a known baseline and regularly monitoring file integrity helps alert you to unwanted or malicious changes to your files sooner. Falling under the earlier mention of the importance of visibility, file integrity monitoring is crucial in keeping track of activity happening within your cloud environment.

threat stack | powered by amazon web services

TOP 10 BEST PRACTICES FOR AWS SECURITY

6 **Implement SSL certificates**
SSL certificates enable encrypted communications between a web server and browser. SSL certificates are issued by Certificate Authorities (CAs), which are organizations that are trusted to verify both the identity and the legitimacy of the entities requesting the certificate.

7 **Harden configuration management**
Configuration management (CM) is an important piece of the DevOps concept of treating infrastructure as code. Since CM execute arbitrary code on infrastructure, you need to harden the systems to protect sensitive data. You can leverage tools such as chef-vault to encrypt sensitive data using public keys or implement file integrity monitoring, as suggested above.

8 **Ensure safe access to production**
If you're practicing continuous delivery, you likely give developers access to production for efficiency purposes. Securing and monitoring activity across production servers is critical. You should be monitoring for events that could be suspicious, such as package installations and updates, to ensure that your CM system is the only entity managing your hosts.

9 **Set up security alerting**
You shouldn't have to go looking for something anomalous. Setting up security alerting ensures that the second anomalous behavior is detecting, you're aware of it. The key to useful security alerting is customization. By assigning different severity levels to different types of alerts, you can clear the clutter and hone in on anomalous, and possibly malicious activity.

10 **Educate employees**
Implementing security protocols is only useful when your employees understand how and why to use them. Employees should know the security risks associated with the business they do. When you execute a new security practice such as multi-factor authentication, you should educate your employees on why it's so important and how to use it.

For a more in-depth analysis, check out Threat Stack's blog post on the subject: blog.threatstack.com.

threat stack | powered by amazon web services

THREAT STACK'S CLOUD SECURITY PLATFORM

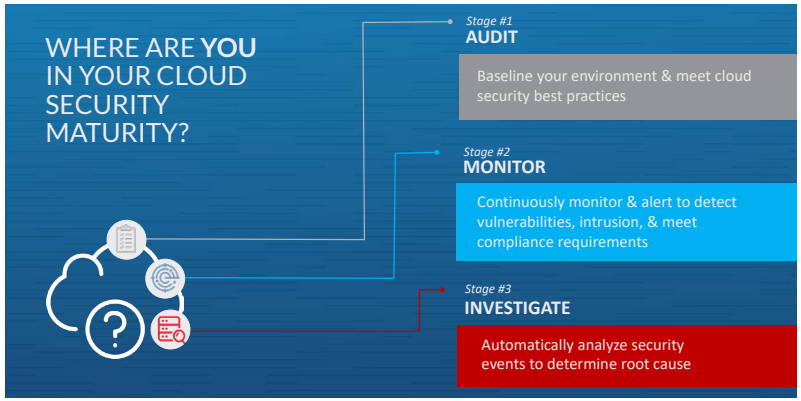
Threat Stack is a comprehensive SaaS security platform that protects your modern infrastructure against external attacks, insider threats, and data loss so you can ensure security and compliance.

Audit Your Environment

Configuration Auditing
Automatically scan your AWS configurations to ensure that the proper security safeguards are active and working properly, while achieving a security baseline.

AWS CloudTrail Alerting
Bridge the gap between your AWS services and the core systems running in your environment. Get alerted on changes to instances, security groups, Amazon S3 buckets, and access keys.

Workflow Integrations
Leverage out-of-the-box integrations with common alerting and configuration management tools. These automatic integrations allow you to seamlessly implement security best practices into your existing DevOps processes.



threat stack | powered by amazon web services

THREAT STACK'S CLOUD SECURITY PLATFORM

Monitor and Alert

Host Intrusion Detection
Understand the difference between normal and suspicious behaviors in your environment, and receive alerts only for the events you need to know about.

Vulnerability Assessment
Detect systems and packages containing known vulnerabilities and cross-reference them against more than 2,000,000 identified CVEs. Threat Stack automatically categorizes them by security risk and shows you which servers are affected by which vulnerabilities.

File Integrity Monitoring
Get alerted when files are accessed or altered by unauthorized users to protect critical customer data, intellectual property, passwords, and credentials.

User Activity Monitoring
Continuously monitor, alert, and build audit trails on all user activity. You can identify abnormal user activity in real time to protect your organization against zero-day and insider threats.

Investigate and Resolve

User Session Playback
Replay a user's session on your application or website. Once you are alerted to an anomalous event, you're able to review the session to pinpoint exactly when and where the event occurred.

Threat Intelligence
Threat Stack monitors connections to known bad addresses so they can notify you immediately when a connection like this occurs.

threat stack | powered by amazon web services

GENESYS' CLOUD SECURITY JOURNEY

Genesys, a global provider of cloud services for customer engagement, communications, and collaboration, decided to transition their applications and workloads over to Amazon Web Services (AWS) and leveraged services such as Amazon Elastic Compute Cloud (Amazon EC2), Amazon Simple Storage Service (Amazon S3), AWS CloudTrail, Elastic Load Balancing, and Amazon Relational Database Service (Amazon RDS) for greater scalability, flexibility, and simplified management. The new environment, supporting Genesis' PureCloud solution, was 100% cloud-native and microservice-based.

"Threat Stack saved us hours previously spent chasing down security events, eliminating the need to hire another security resource"

Reducing Time to Security Incident Detection

While this transition brought efficiency, flexibility, and scale benefits to the organization, the operations and security teams now faced the challenge of ensuring complete security and compliance across an ever changing environment.

Adopting Threat Stack, Genesys immediately gained visibility into what happens when a new microservice is deployed. The customized solution that helped Genesys understand the environment's "normal" baseline so that when there is anomalous activity, or something changes, users are notified immediately. The deep visibility that the Genesys security team gained helps them to decrease time to detection across their environment, as well as resource requirements, and hours spent chasing down security events across a complex environment. As a result, they eliminated the need to hire another full-time security person.

AWS enabled Genesys to be more agile and cost-efficient, while Threat Stack helped decrease the time to resolution of security incidents.

threat stack | powered by amazon web services

MORE INFORMATION

About Threat Stack

Threat Stack enables growth-driven companies to scale with confidence by identifying and verifying insider threats, external attacks and data loss in real-time. The only fully integrated, cloud-native security platform that gives customers instant visibility and automatically responds to changes in their environment throughout the stages of their cloud security maturity, from auditing their environment, to continuous monitoring and alerting, to investigation and remediation. Threat Stack provides the coverage needed to run secure and compliant, in all environments, without sacrificing speed and efficiency. For more information, or to start a free trial, visit threatstack.com.

About Amazon Web Services

For 10 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers more than 90 fully featured services for compute, storage, databases, analytics, mobile, Internet of Things (IoT) and enterprise applications from 42 Availability Zones (AZs) across 16 geographic regions in the U.S., Australia, Brazil, Canada, China, Germany, India, Ireland, Japan, Korea, Singapore, and the UK. AWS services are trusted by millions of active customers around the world monthly — including the fastest growing startups, largest enterprises, and leading government agencies — to power their infrastructure, make them more agile, and lower costs. To learn more about AWS, visit aws.amazon.com.

Additional Resources

Threat Stack APN Partner Page

Threat Stack in AWS Marketplace

Webinar: Best Practices for Scaling Securely in AWS

Getting Started with DevOps Security

DevOps Security Playbook

Genesys Case Study