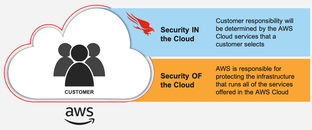
CROWDSTRIKE | aws

5 BEST PRACTICES FOR ENHANCING SECURITY FOR AWS WORKLOADS

As cloud adoption accelerates, cloud security risks are growing more complex and sophisticated. According to CrowdStrike's 2021 Global Threat Report, in just two years, there has been a fourfold increase in the number of interactive intrusions.

As threat actors constantly test new techniques, it's important to keep pace. Maintaining a robust security posture and adopting innovative security solutions that employ advanced techniques is more imperative than ever.

While AWS is responsible for maintaining the security and reliability of its services and the underlying infrastructure that support them, it is ultimately up to the customer to ensure the workloads hosted on AWS remain secure. The following 5 security best practices will help bolster protection for your AWS workloads, mitigate the risk of cyberattacks, and enhance the security of your cloud environment.



1 EVALUATE YOUR CAPABILITIES

A fundamental starting point for securing your AWS workloads is to better understand your current cloud security posture. Start by pinpointing any potential misconfigurations in your cloud environment that could impact security, highlighting weak security policies, and looking for vulnerabilities in your environment that could leave your organization susceptible to a breach.

2 SIMPLIFY YOUR ARCHITECTURE

Traditional security architectures have become overly complex and cannot easily adapt to the cloud. Every new security problem has required a new tool to solve it, leading to intricate and oftentimes complicated security stacks. This complexity poses its own security risks. To mitigate these risks, choose a cloud-native security solution that simplifies your security architecture and enables your organization to tap into the agility and scalability of the cloud while enhancing security.

3 ATTAIN END-TO-END VISIBILITY

As security threats become more intricate, advanced, and difficult to detect, maintaining end-to-end visibility for your environment is a must. Leverage a security solution that offers a single-pane-of-glass view to provide the 360-degree situational awareness necessary for strategic decisions regarding security and resources. Maintaining broad visibility of your environment enables your organization to discover – and remediate – threats that may have otherwise gone undetected.

4 EVOLVE DEFENSE TECHNIQUES

Too many organizations are focusing on malware alone. Meanwhile, attackers have evolved beyond malware strategies and are using new techniques to bypass common defense and access business-critical assets. Having a malware-centric strategy may leave organizations blind – and unprepared – to protect themselves against more complex threats.

5 AUTOMATE SECURITY TASKS

Manually gathering security data and trying to determine how events are related can be time consuming and cumbersome. In addition, critical anomalies and correlations may be hard to discover with manual analysis. With the CrowdStrike Falcon Platform, customers can automate operational tasks to make workloads efficient and secure from deployment to termination. Automatic detection of attacker behavior with prioritized alerts eliminates time-consuming manual assessments.

CrowdStrike's unique combination of technology, threat intelligence, and expertise comes together in a comprehensive platform for protecting your AWS workloads. The CrowdStrike Falcon Platform is an industry-leading, cloud-native security solution, solving a variety of security issues while eliminating cost and complexity.

Together, Falcon and AWS seamlessly integrate security into cloud workloads and provide a sweeping, real-time view of critical security alerts. The CrowdStrike and AWS integrations empower your entire team to evaluate existing security capabilities, simplify architecture, attain end-to-end visibility, evolve defense techniques, and automate security tasks, making it easy for organizations to uphold the shared responsibility model and bolster protection for AWS workloads.

Download the eBook

CROWDSTRIKE | aws

WE STOP BREACHES