CrowdStrike Guide

CROWDSTRIKE

QUICK START GUIDE TO SECURING CLOUD-NATIVE APPS

QUICK START GUIDE TO SECURING CLOUD-NATIVE APPS

Today's application lifecycle places a premium on speed, requiring cloud teams to build cloud-native applications supported by a programmable infrastructure that enables businesses to change and reconfigure their cloud infrastructure on the fly. Additionally, continuous integration/continuous delivery (CI/CD) introduces ongoing automation and continuous monitoring throughout the application lifecycle — from integration and testing, to delivery and deployment — resulting in faster innovation.

As you migrate to the cloud, understanding the blocking and tackling of security is one of the most important factors you should consider. You'll be sharing and/or storing company data with your chosen service provider.

To ensure your data is secure, there are numerous security factors to consider, from shared responsibility to whether the provider's security standards meet your requirements. This can be overwhelming, especially if you're not a security expert.

To help, we've compiled a quick start guide for securing cloud-native applications.

1. **Enforce MFA on the root user and IAM users:** Multifactor authentication (MFA) is an essential step in securing a cloud environment. This can help deter attackers that are able to compromise credentials to the environment but are unable to compromise the MFA device associated with them. Additionally, in AWS, MFA on the root user makes the account harder to recover by attackers, adding even more security.

2. **Enforce a strong IAM password policy:** Strong password policies can prevent users from being compromised through leaked hashes or brute force attacks. A strong password is essential to the basic security of a cloud environment.

3. **Enable global API logging:** Enabling services like AWS CloudTrail is crucial to the security of a cloud environment. This allows you to track, react to and store all of the events going on in your cloud environment.

4. **Use the appropriate secret management services for secret storage:** Services such as AWS Systems Manager Parameter Store and AWS Secrets Manager allow you to securely store and retrieve secret values. These types of services should be used over storing secrets directly in code, environment variables or other places where they may be viewed in cleartext.

5. **Use encryption everywhere:** Some cloud providers, like GCP, enforce encryption everywhere by default, but others do not. For compliance and security, data at rest and in transit should be encrypted with the proper controls provided by the cloud service provider.

6. **Enable and monitor security monitoring services:** Services like AWS GuardDuty or GCP Event Threat Detection identify when potentially malicious activity in an environment is taking place. These services should be enabled and properly monitored to ensure malicious activity is identified.

7. **Back up automatically *and* manually:** It is important to utilize automatic and manual backups for data services, such as AWS Simple Storage Service (S3), AWS Relational Database Service (RDS) and AWS Elastic Block Store (EBS). Automatic backups ensure that data is routinely backed up without user interaction, while manual backups provide additional assurance that data is not lost if something were to happen to the automatic backups.

8. **Utilize the principle of least privilege:** By granting users only the necessary permissions to perform their job duty and nothing else, you can ensure that the blast radius of a compromised account is minimized. Additionally, the principle of least privilege reduces risk against insider threats and even the risk of accidental API calls that could potentially be destructive.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 4 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

CROWDSTRIKE CLOUD SECURITY

Think It, Build It, Secure It

FALCON CLOUD WORKLOAD PROTECTION

Provides comprehensive breach protection across private, public, hybrid and multi-cloud environments, allowing customers to rapidly adopt and secure technology across any workload.

FALCON HORIZON™

Provides multi-cloud visibility, continuous monitoring, and threat detection, and ensures compliance, enabling DevOps to deploy applications with greater speed and efficiency — it's cloud security posture management made simple.

CONTAINER SECURITY

Accelerates critical detection, investigation and threat hunting tasks performed on containers — even on ephemeral containers after they have been decommissioned — enabling security teams to secure containers at the speed of DevOps without adding friction.

CLOUD SECURITY ASSESSMENT

Allows you to test and evaluate your cloud infrastructure to determine if the appropriate levels of security and governance have been implemented to counter inherent security challenges.