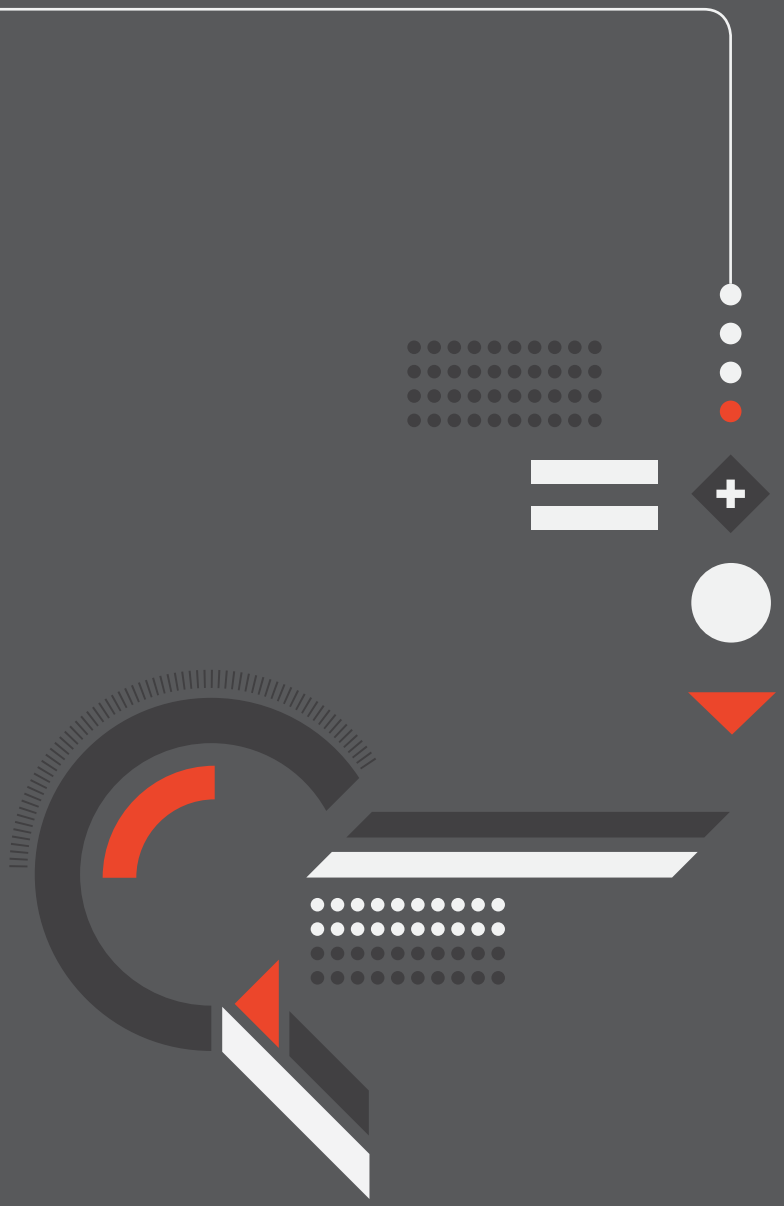
eBook

CROWDSTRIKE CLOUD SECURITY ON AWS

CROWDSTRIKE | aws

TABLE OF CONTENTS



INTRODUCTION

All over the globe, cloud technology is powering organizations of every size, and increasingly, businesses are building on or migrating to Amazon Web Services (AWS). Business requirements like flexibility, innovation, and TCO are driving CTOs and CIOs to adopt AWS technologies. These executives trust AWS to help them respond to changes with speed and confidence, scale effectively, and drive business growth.

As businesses evolve, so too must security strategies to stay one step ahead of threats. Having a cloud security strategy in place early is key to being prepared for anything as technology and cyber-attacks become more sophisticated.

Whether your business is built on the cloud, or you are in the middle of your cloud adoption journey, thinking through your cloud security strategy is critical. No matter what stage you're at, securing your compute should be front of mind.

In an evolving landscape of cloud technology where change is a constant, there's one thing we can guarantee: adversaries understand the security risks of the cloud. Do you?

52%

The percent of North American Organizations which expect at least 41% of their workloads to operate on the cloud in the next 24 months

STAYING SECURE ON THE CLOUD MIGRATION JOURNEY

Cloud technology has helped new businesses launch with speed. It's helped current companies create foundations for innovation and prompted a new set of security parameters and threats. But innovation can also include risks such as decentralized development and policy implementation, visibility gaps across various techs and endpoints, and the ever-dangerous human factor—in other words, shadow IT, poorly built architecture, and lack of knowledge and skill.

For businesses utilizing cloud technology to build infrastructure and scale at will, security means ensuring protection across a constantly changing environment. Outsourced apps and solutions built by third parties with various security standards and architecture can leave security gaps. So, implementing a security strategy early is the best way to maintain centralized visibility into various cloud components and services.

For those migrating to the cloud from legacy tech, security risks are present in systems both new and old. Hybrid solutions during a migration are particularly vulnerable, as are older systems and databases left behind, if not disposed of properly. Most migrations also mean retraining or hiring new employees and a company culture shift. While this creates a good foundation for handling future technology changes, it can also rock the boat. Thus, maintaining a top-down view of security in the midst of a major technology transition is critical.

CROWDSTRIKE'S STRATEGIC SECURITY APPROACH

One way to secure your cloud systems is to engage a security partner like CrowdStrike. With the CrowdStrike Falcon Platform and support from a team of cybersecurity experts, you can be sure your systems are protected on all fronts and no attack will go unseen.

The CrowdStrike Approach:

- Focus on the adversary
- Reduce exposure
- Monitor attack surface
- Protect at runtime
- Be apart of the CI/CD pipeline

Adversaries have adapted attacks common elsewhere in the IT landscape such as permissions escalating, ransomware, and data and packet sniffing to the cloud. New cloud-native attack techniques are likely to emerge as well. CrowdStrike's cloud security solutions have real-time alerting and reporting on 150+ cloud adversaries directly built in, so when new threats emerge, you'll be ready to respond.

In cloud security, reducing exposure and shrinking your attack surface means segmenting workloads, tying up loose ends (especially for those leaving old systems behind), and making sure security is a first consideration when utilizing the cloud, also known as shifting left. With the attack surface defined, high-visibility monitoring is the best way to defend against would-be attackers. CrowdStrike's Falcon Platform features automated analysis, runtime and at-rest protection, cloud native indicators of attack (IOAs), and machine learning for improved investigation speed.

Falcon Horizon for DevSecOps and Monitoring

For those building across multiple environments, CrowdStrike's Falcon Horizon streamlines posture management with a single source of truth for all cloud assets and security configurations. Everything you need to see, all in one place. With IOA protection and ML-based guided remediation built directly into the control plane, Falcon Horizon helps teams to manage compliance and securely rollout AWS integrations with greater efficiency.

Falcon Cloud Workload Protection (CWP) for Comprehensive Breach Prevention

As you build or replace systems with cloud technology, Falcon CWP provides comprehensive breach protection across private, public, hybrid and multi-cloud environments, allowing customers to rapidly adopt and secure technology across any workload. With Falcon CWP, you can build, run, and secure applications with speed and confidence.

SECURING CONTAINERS ON AWS

Ensuring your containers are secure is another key element of an effective cloud security strategy. Isolated and independent by nature, containers limit visibility. Often, they're built with a "set-and-forget" mentality, leaving long-term security compliance as an afterthought. But even with the best monitoring practices, containers can cause trouble in security analysis due to the sheer amount of data they produce in vulnerability scanning.

CrowdStrike's Falcon Platform tackles these issues head on. Falcon CWP's lightweight agent provides complete visibility into containers whether they're on-premises or cloud deployments. Continuous monitoring and CI/CD pipeline integration make it easy to check up on containers and reset them as needed. Additionally, Falcon CWP's monitoring and automated continuous threat detection provides nimble AI/ML vulnerability data analysis at massive scale as well as runtime protection with real-time alerts.

SECURING YOUR COMPUTE ON AWS IS SIMPLE AND EASY WITH FALCON

Organizations who build on AWS know the value of cloud technology for migrating outdated systems and building modern applications. They also know the value of partnering with companies at the forefront of technology to power their systems and grow their business.

The CrowdStrike Falcon Platform seamlessly integrates with AWS Security Hub, is built with AWS services like Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Service (Amazon ECS), and Amazon Linux 2 in mind, and deploys through AWS Systems Manager. AWS customers who partner with CrowdStrike get up and running in minutes and instantly have access to insights and analysis of all their services in one central console. In addition, CrowdStrike Falcon CWP and Horizon both operate with a tiny footprint, leaving zero impact on runtime performance even when analyzing, searching, and investigating.

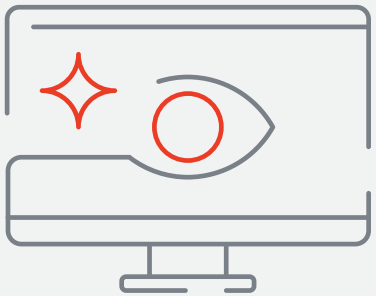
Where AWS and CrowdStrike Work Together

CrowdStrike & AWS compute services

- Containers workloads
- Amazon EC2 instances – including Graviton
- Amazon WorkSpaces
- Amazon Elastic Kubernetes Service
- Amazon Elastic Container Service
- AWS Fargate

CrowdStrike & AWS Cloud services integrations

- AWS Control Tower
- AWS Security Hub
- AWS Systems Manager
- AWS PrivateLink
- Amazon GuardDuty
- AWS Network Firewall
- AWS CloudEndure Disaster Recovery



THE TIME TO BUILD A CLOUD SECURITY STRATEGY IS NOW

When it comes to cloud security, partnering with an expert who understands your adversaries, what they're after, and how they attack is the best way to defend your business against them. As an industry leader in cybersecurity, CrowdStrike has a proven track record of preventing breaches.

For more information on CrowdStrike and AWS solutions, visit:

CrowdStrike Falcon for AWS ›

Upcoming CrowdStrike and AWS events ›

CrowdStrike and AWS partner page ›

CrowdStrike on AWS Marketplace ›