CROWDSTRIKE

# FALCON HORIZON CLOUD SECURITY POSTURE MANAGEMENT

Stop cloud breaches in their tracks with unified visibility, threat detection and continuous monitoring and compliance for multi-cloud environments

## SEE MORE, KNOW MORE, DO MORE

The adoption of the cloud has fundamentally changed how businesses go to market and develop modern applications. Today's application development lifecycle places a premium on speed to market, requiring development teams to build cloud-native applications supported by a programmable infrastructure that enables businesses to change and reconfigure the cloud infrastructure on the fly.

This shift presents new challenges that make it difficult for security teams to keep up. The result is poor visibility and control of cloud resources, fragmented approaches to detecting and preventing misconfigurations, an increasing number of security incidents and the inability to maintain compliance.

Falcon Horizon streamlines cloud security posture management across the application development lifecycle for any cloud, enabling you to securely deploy applications in the cloud with greater speed and efficiency. The CrowdStrike Falcon® cloud-native platform provides visibility into your entire cloud infrastructure, continuous monitoring for misconfigurations, and proactive threat detection — allowing DevSecOps teams to fix issues faster and be more productive.

## KEY BENEFITS

- Provides complete multi-cloud visibility with a single source of truth for cloud resources
- Prevents cloud misconfigurations and application vulnerabilities
- Reduces alert fatigue and enables you to remediate issues faster
- Delivers agentless cloud-native protection

FALCON HORIZON
CLOUD SECURITY POSTURE MANAGEMENT

# KEY CAPABILITIES

## DISCOVERY AND VISIBILITY

Provides discovery and visibility into cloud infrastructure and resources:

- Access a single source of truth for cloud assets and security configurations across multi-cloud environments and accounts.
- Discover cloud resources and details automatically upon deployment, including misconfigurations, metadata, networking, security and change activity. Supported services include: AWS: EC2, ELB, RDS, S3, IAM, EBS, VPC and KMS; and Azure: Virtual Machine, Load Balancer and Storage Accounts.
- Manage security group policies across accounts, projects, regions and virtual networks from a single console.
- Identify cloud resources not protected by Falcon Horizon.

## MISCONFIGURATION MANAGEMENT AND REMEDIATION

Eliminates security risks and accelerates the delivery process:

- Compare cloud application configurations to industry and organizational benchmarks, to identify violations and remediate in real time.
- Fix issues that leave cloud resources exposed — such as misconfigurations, open IP ports and unauthorized modifications — with guided remediation and guardrails that enable developers to avoid critical mistakes.
- Monitor storage to ensure permissions are secure and not publicly accessible.
- Monitor database instances and verify that high availability, backups and encryption are enabled, as well as security groups to limit exposure.

## CONTINUOUS THREAT DETECTION

Proactively detects threats across the application development lifecycle:

- Cut through the noise of multi-cloud environment security alerts with a targeted threat identification and management approach.
- Drastically reduce the number of alerts by focusing on areas adversaries are most likely to exploit.
- Prioritize vulnerabilities based on your environment and prevent vulnerable code from reaching production.
- Continuously monitor for malicious activity, unauthorized behavior and access to cloud resources using real-time threat detection.

## DEVSECOPS INTEGRATION

Employs cloud-native, agentless posture management to reduce overhead and eliminate friction and complexity across multi-cloud providers and accounts:

- Gain centralized visibility and control over all cloud resources to ensure security operations and DevOps teams have a single source of truth.
- Enable security teams to prevent compromised assets from progressing down the application lifecycle.
- With SIEM integration, streamline visibility for security operations and provide insights and context into misconfigurations and policy violations.
- Using the single API, achieve faster integration, remediation and response within the DevOps tool sets you already use.
- Through reporting and dashboards, drive alignment and a shared understanding across security operations, DevOps and infrastructure teams.



## ELIMINATE SECURITY BLIND SPOTS WITH FALCON HORIZON

**Unifies visibility and control across multi-cloud environments:** Falcon Horizon delivers continuous discovery and visibility of cloud-native assets, providing valuable context and insights into the overall security posture and the actions required to prevent potential security incidents.

**Prevents cloud misconfigurations:** Falcon Horizon provides intelligent monitoring of cloud resources to proactively detect misconfigurations, vulnerabilities and security threats, along with guided remediation to resolve security risks and enable developers with guardrails to avoid costly mistakes.

**Reduces alert fatigue with targeted threat detection:** Falcon Horizon continuously monitors for anomalies and suspicious activity, and integrates seamlessly with SIEM solutions, enabling security teams to gain visibility, prioritize threats, reduce alert fatigue by eliminating noise, and respond and fix issues faster.

## ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), 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 3 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.