

## FALCON CLOUD SECURITY SOLUTION BRIEF:

# 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.

CrowdStrike Falcon® Cloud Security 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 cloud-native CrowdStrike Falcon® 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 automatically

---

Assesses the security of cloud accounts and eliminates compliance violations

---

Reduces alert fatigue and accelerates incident response

---

Improves code quality and shortens release cycle times

---

Delivers agentless cloud-native protection

# KEY CAPABILITIES

## DISCOVERY AND VISIBILITY

Unify visibility and security enforcement across multi-cloud and on-premises environments in a single cloud-native solution.

- **Single source of truth:** Get up and running in minutes and access a single source of truth for all cloud assets and security configurations across multi-cloud environments and accounts.
- **See everything:** Discover cloud resources and details automatically upon deployment — including misconfigurations, metadata, networking security, access control and change activity — and eliminate security blind spots. Supported services include:

AWS		
ACM	EKS	RDS
API Gateway v1	ElastiCache	Redshift
CloudTrail	ELB	Route 53
CloudFront	EMR	S3
CloudFormation	GuardDuty	SES
Config	IAM	SNS
DynamoDB	Kinesis	SQS
EBS	KMS	SSM
EC2	Lambda	VPC
ECR	NLB/ALB	

Azure	
Active Directory (AD)	Load Balancer
App Service	Monitor
Container Registry	Network Security Groups
Disk	PostgreSQL
File Service	SQL Server Virtual Machine
Identity and Access Management (IAM)	Storage Account
Key Vaults	Virtual Machine
Kubernetes Service	Virtual Network

GCP	
App Engine	Cloud Storage
BigQuery	Compute Engine
Cloud Load Balancing	IAM
Cloud Logging	KMS
CloudSQL	VPC

- **Simplified management and security policy enforcement:** Manage and enforce security group policies across accounts, projects, regions and virtual networks from a single console to reduce the attack surface.
- **Monitor the control plane:** Scale at will and gain insight into all control plane API calls and uncover security risks within managed Kubernetes clusters.
- **Identify unprotected resources:** Identify cloud resources not protected by the Falcon agent and take immediate action.

## ELIMINATE SECURITY BLIND SPOTS WITH FALCON CLOUD SECURITY

**Unifies visibility and control across multi-cloud environments:** Falcon Cloud Security 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 and eliminates compliance violations:** Falcon Cloud Security 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 and ensure compliance across multi-cloud environments.

**Reduces alert fatigue with targeted threat detection:** Falcon Cloud Security 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.



## CLOUD SECURITY POSTURE MANAGEMENT

### MISCONFIGURATION MANAGEMENT AND REMEDIATION

Prevent risky cloud misconfigurations based on CrowdStrike best practices.

- **Eliminate misconfigurations and compliance violations:** Compare cloud application configurations to industry and organizational benchmarks to identify violations and remediate in real time and ensure application availability.
- **Get guided remediation from security experts:** 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.
- **Enforce permissions:** Monitor storage to ensure permissions are secure and not publicly accessible.
- **Prevent identity-based threats:** Reduce the number of tools required from three to one, and prevent users from putting your organization at risk by automating the detection and remediation of identity-based risks in Microsoft Azure, AWS and GCP.
- **Secure Azure AD:** Ensure Azure AD groups, users and apps have the correct permissions using the new Identity Analyzer reports.
- **Reduce alert fatigue:** Remediate issues faster and reduce SOC costs with enhanced policy management for cloud accounts, regions or specific resources.
- **Ensure resilience:** Monitor database instances and verify that high availability, backups and encryption are enabled, as well as security groups to limit exposure.

### REAL-TIME THREAT DETECTION

Continuously detect, prevent and remediate cloud control plane security threats to stop breaches.

- **Accelerate response:** Reduce the time it takes to detect and mitigate a breach from months to minutes by cutting through the noise of multi-cloud environment security alerts with an adversary-focused approach that saves time and allows teams to take the most effective action.
- **Identify malicious activity with confidence scoring and prioritization:** The patent-pending Confidence Scoring in Falcon Cloud Security continuously aggregates, assesses and scores control plane threats and configurations to accurately identify malicious activity, reducing the time to understand and respond.
- **Integrate cloud indicators of attack (IOAs) with threat intelligence:** Gain access to real-time alerting and reporting on over 150 cloud adversaries based on CrowdStrike's market-leading threat intelligence and research for more effective response.
- **Benefit from continuous control plane threat detection:** Machine learning and behavior-based TTP/IOA detections and guided remediation are provided for all cloud accounts, services and users across the cloud estate, improving investigation speed by up to 88%.
- **Enable self-service threat hunting:** Cloud-scale data and analytics for all cloud activity enable security teams to proactively uncover hidden threats and take action.

## CLOUD SECURITY POSTURE MANAGEMENT

### CONTINUOUS COMPLIANCE MONITORING

Assess the security of cloud accounts and eliminate costly compliance violations.

- **Continuously monitor compliance:** Continuously monitor the compliance posture of all of your cloud resources from a single console.
- **Assess for CIS benchmarks:** Assess the security of cloud accounts against Docker and Kubernetes CIS benchmarks with 250 out-of-the-box, adversary-focused policies to save time and reduce operational costs.
- **Ensure audit-ready compliance:** Continuously monitor the compliance of all of your cloud resources and avoid costly fines using a single console for regulations, including PCI, NIST and more.
- **Eliminate compliance violations:** Identify policy violations and take immediate user-driven action to remediate.

### DEVSECOPS INTEGRATION

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

- **Improve decision making:** With SIEM integration, streamline visibility for security operations and provide insights and context into misconfigurations and policy violations for faster incident response.
- **Integrate at the speed of DevOps:** Using the single API, achieve faster integration and remediation within the DevOps and collaboration tools you already use, such as email, Slack, PagerDuty and more.
- **Fuel business performance:** Through reporting and dashboards, drive alignment and a shared understanding across security operations, DevOps and infrastructure teams.

### ABOUT CROWDSTRIKE

**CrowdStrike** (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more:

<https://www.crowdstrike.com/>

Follow us: [Blog](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

© 2023 CrowdStrike, Inc. All rights reserved.

