

Falcon Cloud Security

Secure your cloud with speed, visibility and unrivaled detection and response

The Need for Security Consolidation

Cloud security is complex, with an increasing number of workloads and containerized applications across hybrid and multi-cloud environments. Organizations often work with multiple fragmented tools and controls, creating security silos. This leads to poor visibility and inconsistent security policies across the cloud estate. These factors significantly slow down detection and response and create security gaps that adversaries can exploit.

The Adversary Problem

According to the [CrowdStrike 2023 Global Threat Report](#), from 2021 to 2022, cloud exploitation cases grew by 95%, over one-third (36%) of observed cloud environments had insecure cloud service provider default settings, and cases involving threat actors specifically targeting cloud environments nearly tripled. Adversaries are taking advantage of any gaps or vulnerabilities in the attack surface, and a new approach to cloud security is needed.

CrowdStrike's Unified Cloud-Native Application Protection Platform

CrowdStrike Falcon® Cloud Security is the industry's only unified cloud-native application protection platform (CNAPP), which integrates agent-based and agentless protection to stop adversaries, prevent human error and meet compliance needs across all major clouds, workloads and operating systems to stop cloud breaches.

Key Benefits

Use a unified agent-based and agentless platform to stop cloud breaches at runtime and minimize the risk of misconfigurations and human error for any cloud environment

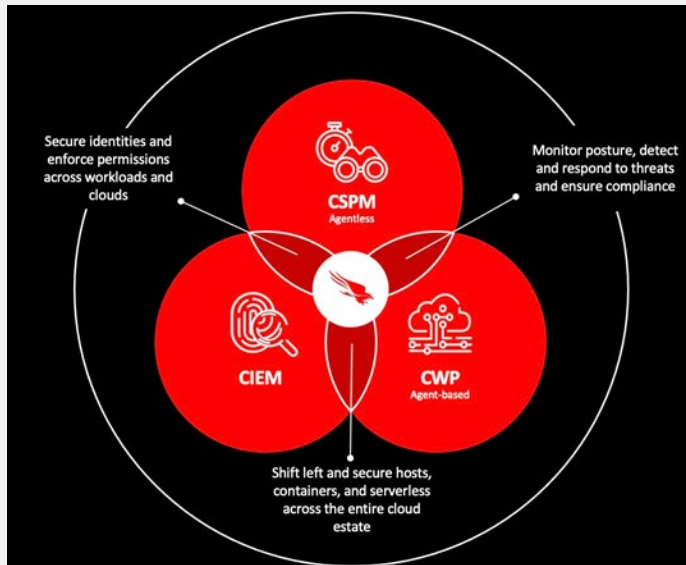
Move faster than the adversary with protection powered by CrowdStrike's industry-leading threat intelligence spanning 200+ adversaries

Solve the cybersecurity skills gap with expert services across threat hunting, incident response and managed detection and response (MDR)

Gain unrivaled identity-based security, visibility and simplified privileged access management and policy enforcement.

Perform one-click remediation testing prior to deployment, and integrate and remediate at the speed of DevOps.

Be prepared to respond to current and future threats with the industry's first 24/7 MDR for cloud, and expert services like cloud threat hunting and incident response



Benefit	Details
World's best adversary intelligence built into a cloud security platform	<ul style="list-style-type: none"> Ability to respond faster than adversaries by using industry-leading adversary intelligence Ability to understand risks so you can proactively resolve them using cloud-specific indicators of misconfiguration (IOMs) to reduce the cloud attack surface Cloud-specific indicators of attack (IOAs) sourced from adversary intelligence to prevent runtime attacks
Industry's only unified agent-based and agentless approach to cloud security for complete visibility and protection	<ul style="list-style-type: none"> One platform to shut down misconfigurations, accidental exposure and human error while stopping active cloud breaches in runtime Protection across all hybrid and multi-cloud platforms, including major Windows, Linux, container and serverless technologies The world's most deployed cloud workload protection (CWP) platform — easy to deploy, no reboot and works almost everywhere — based on 10+ years of leadership in endpoint detection and response (EDR)
Only cloud security vendor to provide services for security response, platform deployment and 24/7 support	<ul style="list-style-type: none"> The only vendor to provide cloud threat hunting and response The industry leader in incident response and professional services for cloud security 24/7 MDR service that can run cloud security or supplement an existing SOC

Technical Solution

Falcon Cloud Security offerings include:

- **Falcon Cloud Security:** Breach protection including threat intelligence, detection and response, workload runtime protection and cloud security posture management across AWS, Azure and GCP.
- **Falcon Cloud Security for Containers:** Includes the features and capabilities of Falcon Cloud Security and adds container and Kubernetes protection. It can be deployed across on-premises, hybrid and multi-cloud environments.
- **Falcon for Managed Containers:** Container security and runtime protection for cloud service providers' managed containers, including threat intelligence, detection and response, container image security and Kubernetes protection.

What's New

- **One-Click XDR:** With this industry-first innovation, organizations can sweep their cloud environment with native agentless visibility to identify unprotected workloads and automatically deploy the CrowdStrike Falcon agent for end-to-end protection. Only CrowdStrike can identify unprotected cloud workloads and automatically protect them with industry-leading extended detection and response (XDR) and EDR for consistent, complete breach prevention.

CrowdStrike Products

Falcon Cloud Security

- **Agentless Snapshot Scanning:** When an agent can't be installed, organizations can gain full visibility into cloud workloads by detecting vulnerabilities and installed applications with native agentless snapshot capabilities — starting with support for AWS.
- **Complete Cloud Attack Path Visualization:** Leveraging CrowdStrike Asset Graph, organizations can see a unified view of the entire path an attacker can take, from host to cloud, to compromise a cloud environment. Only CrowdStrike consolidates real-time data from native agent-based and agentless capabilities to enable organizations to prioritize and reduce risks facing their cloud environment.
- **Compliance Dashboard:** A single dashboard for all common compliance frameworks (NIST, SOC2, PCI and CIS) includes drill-down capabilities to support auditing. Only CrowdStrike provides one compliance dashboard for all cloud environments in a single platform that covers cloud and endpoint.
- **Kubernetes Admission Controller:** Prevent misconfigured containers from deploying. Only Falcon Cloud Security works out-of-the-box without the need for complex Rego rules, saving security teams time while also preventing misconfigured containers from deploying.
- **Infrastructure as Code (IaC):** More easily scan for vulnerabilities in container images across AWS, Azure and GCP while supporting 10+ IaC platforms to drive a more efficient application life cycle. Only CrowdStrike combines IaC with agent-based and agentless capabilities in one platform.

Features	Falcon Cloud Security	Falcon Cloud Security for Containers	Falcon for Managed Containers
Cloud Control Plane			
Cloud security posture management (CSPM)	✓	✓	✗
Behavioral indicators of attack for cloud	✓	✓	✗
Compliance dashboard	✓	✓	✗
Identity analyzer (CIEM)	✓	✓	✗
Cloud Assets Visibility			
Single unified platform (UI)	✓	✓	✓
Workload Protection			
Cloud workload protection (CWP)	✓	✓	✓
Runtime protection	✓	✓	✓
Agent-based and agentless	✓	✓	✓
Container security	✗	✓	✓
Container image assessment via CI/CD	✗	✓	✓
Image assessment policies	✗	✓	✓
Container assets visibility	✓	✓	✓
Runtime protection (NGAV, EDR)	✓	✓	✓
Drift detection for containers	✗	✓	✓
Kubernetes misconfigurations	✗	✓	✓
Protection for lean OS and serverless containers	✗	✓	✓
Integrations			
AWS	✓	✓	✓
Microsoft Azure	✓	✓	✓
Google Cloud	✓	✓	✓
Registry integrations <small>*please see list on the next page</small>	✗	✓	✓
Licensing			
License	Reserve OR On Demand	Reserve OR On Demand	Reserve OR On Demand

What customers have to say

Read about [CoreWeave](#), a CrowdStrike customer using the Falcon Cloud Security product to [power its cloud security journey](#).

"CrowdStrike's ability to provide an adversarial perspective on cloud attack chains supports the strategic imperative for organizations to update their threat model to include their cloud footprint."
— Doug Cahill, Vice President, Analyst Services and Senior Analyst, Enterprise Strategy Group (ESG)

"CrowdStrike's CNAPP provides a deep and accurate view of the cloud threat landscape that we believe sets them apart from the competition."
— Dave Worthington, GM Security and Risk, Jemena

"The one-click auto remediation testing feature stands out amongst the new CIEM capabilities for CrowdStrike [Falcon] Cloud Security."
— Frank Dickson, Group Vice President, Security and Trust, IDC

"We evaluate it very highly as it provides the best protection for our investment!"
— Large Enterprise Telco

CrowdStrike Products

Falcon Cloud Security

Falcon Cloud Security provides maximum security value for customers and leverages the broadest suite of registry integration in the industry. This is critical to supporting customers that have a preferred toolset already in use so they can continue using it.

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.**

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

Current Registry Integrations	
AWS ECR	Docker Hub
Docker Registry V2	Google Artifact Registry
Google Container Registry	IBM Cloud
JFrog Artifactory	Microsoft ACR
Oracle Container Registry	Red Hat OpenShift
Red Hat Quay.io	Sonatype Nexus
VMware Harbor	Docker Hub
GitLab	

Industry Recognition

CrowdStrike Named a Representative CNAPP Vendor in the 2023 Gartner® CNAPP Market Guide

Tested and proven leader

CrowdStrike is proud to be recognized a leader by industry analyst and independent testing organizations.

THE CHANNEL CO.
CRN
Learn more about how CrowdStrike won the 2022 CRN Tech Innovator Award for Best Cloud Security.
[Read the report >](#)

FROST
&
SULLIVAN
Learn why Frost & Sullivan ranked CrowdStrike as a leader in Cloud-Native Application Security Platform (CNAPP).
[Read the report >](#)

FORRESTER®
CrowdStrike received the highest possible score in the scalability and in the execution roadmap, and among the second highest in the partner ecosystems securing workloads criterion in the 2022 Forrester Wave™ for Cloud Workload Security.
[Read the report >](#)