CROWDSTRIKE

CrowdStrike Products
Soultion Brief

# Falcon Cloud Security:
# Container and Shift-Left Security

Secure hosts, virtual machines, containers and Kubernetes serverless deployments

## Cloud security at the speed of DevOps

Cloud adoption is exploding, as companies realize the potential for the innovation and business agility the cloud offers. The cloud allows organizations to add new resources on demand, from virtual machines to serverless functions to containers. Developers also deploy new code every day in the cloud, which creates new attack surfaces and threats for businesses. As more technologies and architectures are brought into the cloud in pursuit of innovation and growth, the nature of cloud risk grows and becomes more complex.

According to the CrowdStrike 2024 Global Threat Report, there was a **75% increase in cloud intrusions in 2023**, with a 110% increase in cases involving cloud-conscious threat actors. The cloud is rapidly becoming a major battleground for cyberattacks — and the cost of a breach has never been higher. The estimated average cost of a breach impacting multi-cloud environments is more than $4.75 million USD in 2023.[1] Existing approaches to cloud security failed — they provide only siloed views of the cloud, resulting in blind spots; generate noisy alerts that waste security and development teams' time; and require manual effort to correlate disparate data to understand the risk. Businesses need full cloud visibility, including applications and APIs, to eliminate misconfigurations, vulnerabilities and other security threats in real time.

## Key benefits

- Get unified visibility and protection across the entire cloud
- Use a single solution to see and stop cloud attacks
- Shift left and automate DevSecOps

[1] IBM Cost of a Data Breach Report 2023

## How does Falcon Cloud Security help?

CrowdStrike is the first cloud-native application protection platform (CNAPP) vendor to natively secure your business in the cloud by providing complete visibility across cloud and app-level risks. CrowdStrike Falcon® Cloud Security stops breaches faster with the world's only unified agent and agentless approach to cloud security, extending from code to cloud in a single platform. It covers the key areas required for CNAPP with pre-runtime and run-time protection and agentless technology.

CrowdStrike is the only CNAPP vendor with a range of cloud threat detection and response services including incident response, threat hunting, assessment and 24/7 MDR services for your entire cloud estate. Falcon Cloud Security also helps you discover and map your apps and APIs running in production, showing you all attack surfaces, threats and critical business risks.

## A real-life example

Mercury Financial partnered with several legacy security vendors over the years, but the performance just wasn't there. As it tapped into new markets and added new customers, Mercury Financial needed a modern solution that could support the scalability of a cloud-native environment.

Falcon Cloud Security helped Mercury Financial understand its current threat status for cloud workloads and speed up response to incidents and risks by 89%. At the same time, Falcon Cloud Security scanned the company's cloud infrastructure to detect and remediate misconfigurations and vulnerabilities. Mercury Financial also uses CrowdStrike to support its "shift left" strategy to introduce security early in application development, including container scanning and Kubernetes protection. This helps developers accelerate time-to-market of new apps, products and services, and deliver a better and safer customer experience.

"Partners like CrowdStrike allow us to scale quickly, secure our entire infrastructure and bring new products and solutions to market much faster."

– Alex Arango, Head of Cyber Threat Management - Deputy CISO at Mercury Financial

Security is not meant to impede your business goals or slow down your software development. It is meant to enable you to reach those goals safely with minimal risk. Falcon Cloud Security provides complete protection that focuses on business impact. It provides comprehensive coverage and integration, advanced threat detection and response, scalability and performance impact, and shift-left security.

## Key features

- Protection for AWS, Google, Azure, Kubernetes and OpenShift
- **Pre-runtime:**
  - CI/CD Security (Pre-Runtime)
  - Container Image Assessment
  - Image Assessment Policies
  - Infrastructure-as-Code (IaC) Security
  - Registry Integrations
- **Runtime:**
  - Container Asset Visibility
  - Next-Generation Antivirus
  - Endpoint Detection and Response
  - Indicators of Attack (IOAs)
  - Drift Prevention
  - Rogue Container Detection
  - Kubernetes Admission Controller
  - Vulnerability Management
  - One-Click Runtime Protection
  - Cloud Attack Path Visualization
  - Runtime Image Assessment

## Key capabilities

### CI/CD Security (Pre-runtime)

- **Ensure safe delivery:** Create verified image policies to ensure that only approved images are allowed to progress through your pipeline and run in your hosts or Kubernetes clusters.
- **Align security and developers:** Streamline visibility and drive alignment through reporting and dashboards to provide shared understanding across security operations, DevOps and infrastructure teams.
- **Integrate with developer toolchains:** Seamlessly integrate with Jenkins, Bamboo, GitLab and more to remediate and respond faster within the DevOps tool sets you already use.
- **Benefit from the broadest industry image assessment:** Integrate with 16 code registries for more complete coverage and the ability to find vulnerabilities, no matter which registry is being used, through automatically performed malware, secrets and vulnerability detections with software composition analysis (SCA).
- **Improve IaC security:** Easily scan for vulnerabilities in container images across AWS, Azure and Google Cloud Platform (GCP) while supporting 10+ IaC platforms to drive a more efficient application life cycle. CrowdStrike combines IaC with agent-based and agentless capabilities in one platform.

### Container Security

- **Get complete visibility and protection for the container environment:** With CrowdStrike's single lightweight agent, you can secure both Kubernetes and containers running on it. Capture container start, stop, image and runtime information, unidentified and rogue containers, and all events generated inside the container, even if it only runs for a few seconds.
- **Investigate container incidents faster:** Easily investigate incidents when detections are associated with the specific container and not bundled with the host events.
- **Prevent attacks on container environments:** Uncover hidden threats in open-source packages and third-party images to prevent attacks on your container-based applications. Also, protect serverless compute engines such as AWS Fargate.
- **Enforce container immutability (container drift):** Ensure only secure images are allowed to progress through your pipeline and run in your Kubernetes clusters or hosts.
- **Improve container orchestration:** Capture Kubernetes namespace, cluster, pod metadata, process, file and network events.
- **Prevent vulnerable deployment:** Save time with Kubernetes Admission Controllers by using predefined policies to prevent vulnerable deployments.

### Vulnerability Management

- **Get visibility and risk management in a unified platform:** Gain visibility into vulnerabilities and prioritize risk around your cloud workloads, containers, images, registries and Lambda functions.
- **Identify vulnerabilities prior to production:** Improve security and save time by assessing your images prior to production through supported registries or running local image assessment.
- **Monitor continuously:** Identify new vulnerabilities at runtime, including runtime image assessment, and alert and take action without having to rescan images.

## Runtime Security

- **Comprehensive visibility and protection:** Get runtime visibility and protection for Linux and Windows hosts, containers and Kubernetes as well as serverless compute engines like AWS Fargate.
- **The ability to stop cloud breaches:** Identify zero-day threats in real time through CrowdStrike Threat Graph®, the industry's most comprehensive set of endpoint and workload telemetry, threat intelligence and AI-powered analytics.
- **Accelerated response with enriched threat intelligence:** Gain visibility into relationships across account roles, workloads and APIs for deeper context, leading to faster, more effective response.
- **Agentless snapshot scanning:** When an agent can't be installed, organizations can gain full visibility into cloud workloads by detecting malware, vulnerabilities and installed applications with native agentless snapshot capabilities.
- **One-Click XDR:** Scan your 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 endpoint detection and response (EDR) for consistent, complete breach prevention.
- **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 in their cloud environment.

## Managed Detection and Response (MDR) for Cloud

- **24/7 expertise to defend the cloud:** Benefit from the expertise of seasoned security professionals who have experience in cloud defense, incident handling and response, forensics, SOC analysis and IT administration.
- **Continuous human threat hunting:** 24/7 monitoring is provided by the CrowdStrike Falcon® Adversary OverWatch™ team, CrowdStrike's human threat detection engine that hunts relentlessly to find and stop the most sophisticated hidden threats.
- **Surgical remediation:** The Falcon Adversary OverWatch team remotely accesses affected systems to surgically remove persistence mechanisms, stop active processes, clear other latent artifacts and restore workloads to their pre-intrusion state without the burden and disruption of reimaging.
- **Breach Prevention Warranty:** CrowdStrike stands strongly behind its breach protection capabilities by providing a **Breach Prevention Warranty*** to cover costs should a breach occur within the protected environment.

  *Breach Prevention Warranty not available in all regions.

## A high-level overview of Falcon Cloud Security

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

*For a complete list of features and specifications,* ***contact a CrowdStrike cloud security expert.***

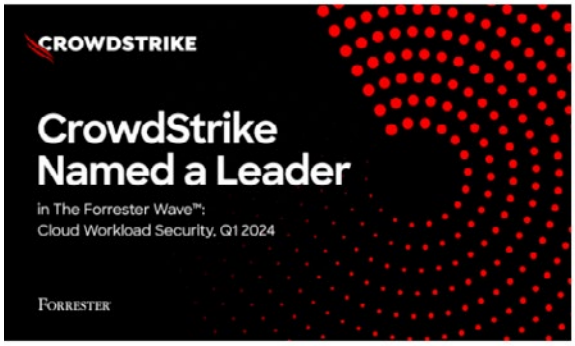
Falcon Cloud Security provides maximum security value for customers and leverages the broadest suite of registry integrations in the industry. This is critical to supporting customers that have a preferred tool set already in use so they can continue using it.

| 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 | Google Artifact Registry |
| GitLab | |

# Industry recognition

CrowdStrike Named a Leader: 2024 Wave for Cloud Workload Security

## A tested and proven leader




### The Forrester Wave™: Cloud Workload Security, Q1 2024

CrowdStrike receives the highest position of all vendors in the Strategy category; receives the highest scores possible in the Vision and Innovation criteria.

**Download Report**

## 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.

**Get a FREE Cloud Security Health Check**