CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Cloud Security

Secure everything across your cloud using the industry's first CNAPP with unified security posture management (USPM) visibility

The attack surface

Attack surfaces are bigger, more ephemeral and harder to manage. CrowdStrike surveyed 400 application security professionals and found that 71% released application updates at least once a day.[1] The complexity of multi-cloud and hybrid cloud environments coupled with the continuous change of modern applications makes it more difficult to secure everything, everywhere, all the time. In addition, organizations need to protect innovations.

The adversaries

According to the CrowdStrike 2024 Global Threat Report, cloud intrusions grew by 75% from 2022 to 2023, and cases involving cloud-conscious threat actors grew by 110% year-over-year.[2] Adversaries are cloud experts, ready to take advantage of any gaps or vulnerabilities in the attack surface.

The silos

Security teams are using multiple fragmented tools. Without a single source of truth, visibility is limited, security policies are inconsistent and teams have an unmanageable number of security alerts to triage, investigate and remediate. These factors significantly slow down detection and response and create security gaps that adversaries can exploit.

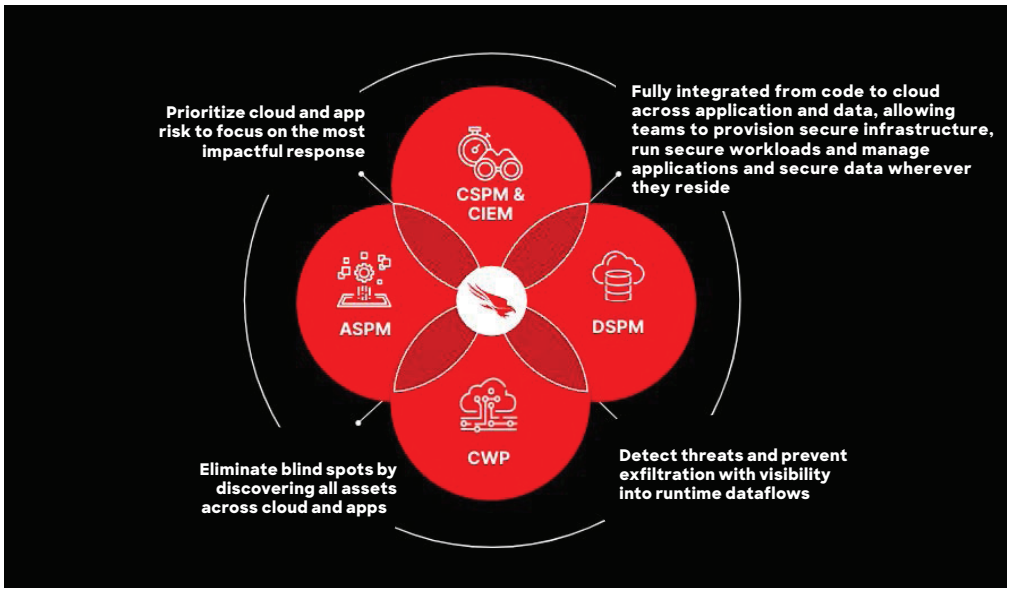
Key benefits

- **USPM-level visibility with the only CNAPP that combines application security posture management (ASPM), data security posture management (DSPM) and AI security posture management (AI-SPM):** Gain a real-time, complete 360-degree view of security posture across multi- and hybrid cloud environments.
- **Continuous security:** Prevent misconfigurations from the start to stop cloud breaches at runtime.
- **Risk-based prioritization:** Reduce alert fatigue and false positives by contextualizing vulnerabilities and weaknesses based on exploitability and impact.
- **Seamless workflows:** Eliminate silos and empower diverse teams to remediate the riskiest issues first.
- **Superior threat intelligence:** Move faster than the adversary with protection powered by CrowdStrike's industry-leading threat intelligence spanning 245+ adversaries.
- **Expertise on demand**: Solve the cybersecurity skills gap with expert services across threat hunting, incident response, and managed detection and response (MDR).

[1] CrowdStrike 2024 State of Application Security Report
[2] CrowdStrike 2024 Global Threat Report

The answer: CrowdStrike's unified cloud-native application protection platform

CrowdStrike Falcon® Cloud Security is the industry's first and only unified cloud-native application protection platform (CNAPP), fully integrated from code to cloud across application and data, allowing teams to provision secure infrastructure, run secure workloads and manage applications and secure data wherever they reside.



Business value for Falcon Cloud Security customers[3]

Benefit	Details
Full visibility	• Gain broad visibility across all cloud infrastructure and applications • Speed cloud estate discovery and monitoring by up to 72%
Risk-based prioritization	• Correlate risk from code to cloud and prioritize threats based on exploitability, likelihood and business impact • Reduce false positives by up to 100x • Save up to 65 hours per month not responding to cloud incidents
Best-in-class prevention	• Drive compliance through out-of-the-box and custom policies • Increase the efficiency of your development and security team by identifying misconfigurations earlier • Gain up to 89% faster cloud detection and response
Powered by industry-leading threat intelligence	• Apply intelligence gathered from the crowd — CrowdStrike tracks 245+ adversaries, and the CrowdStrike Falcon® platform processes 200K new indicators of compromise (IOCs) daily and makes 140+ millions indicators of attack (IOAs) decisions per minute • Elevate your cloud security with a range of services — including cloud threat detection and response, incident response, thread hunting and 24/7 MDR

[3] These numbers are projected estimates of average cost benefit based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on the individual customer's module deployment and environment.

Falcon Cloud Security use cases

Secure Code, Pre-Runtime: Integrated security and tools empower developers to build faster and leverage the tools they like. Fully integrated CI/CD pipeline security lets teams check and validate registries, containers, Kubernetes and code seamlessly pre-runtime.

Secure Your Data and Apps Everywhere with USPM: Gain a 360-degree view of your security posture with Falcon Cloud Security. The integration of DSPM, ASPM and AI-SPM provides true security posture context, delivering unique insight into critical cloud data flows and ensuring applications are secure at every stage.

Secure Cloud Infrastructure with Cloud Security Posture Management (CSPM): Get full and continuous visibility and monitoring across all clouds. Empower teams to provision cloud infrastructure securely, prevent misconfigurations through standardized policies and maintain compliance.

Secure Cloud Access with Cloud Infrastructure Entitlement Management (CIEM): Simplify access control in the cloud. Manage identities and entitlements to prevent identity misconfigurations and improper access that can lead to malicious attacks.

Secure Cloud Workloads with Cloud Workload Protection (CWP): Protect your entire cloud-native stack, on any cloud, across all workloads, containers and Kubernetes applications. Get complete visibility into workload and container events for faster and more accurate detection, response, threat hunting, investigation and remediation.

Secure Your Innovations and AI Models with AI-SPM: Identify misconfigurations and support compliance with regulatory requirements, while AI and machine learning-based detections prevent model poisoning and tampering, helping ensure the reliability of your AI-driven processes.

Secure Cloud Applications with ASPM: Extend security to the applications you build and deploy. Get continuous visibility into every microservice, database, API and dependency to maintain accurate software bills of materials (SBOMs), prioritize application vulnerabilities and protect sensitive data.

Secure Data with DSPM: Automatically discover, classify and prevent data leaks in every state — at rest, in use and in motion.

Secure Your Cloud Faster with Cloud Detection and Response (CDR): Gain visibility, speed, accuracy and protection across your cloud environment with best-in-class CDR to help you understand everything that is happening and outpace the adversaries. This includes tools like attack path analysis to simplify detection and response for SOC teams with a bird's-eye view of a potential attack from end to end, including access to query data logs to enrich and streamline response.

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 Google Cloud.

Falcon Cloud Security for Containers: Includes the features and capabilities of Falcon Cloud Security, and also 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.

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

"Now with CrowdStrike, we can remediate any cloud intrusion in less than 16 minutes, which puts our minds at ease, while ensuring a great user experience for our clients."
— Kevin Tsuei, SVP Information Security Officer, Commercial Bank of California

"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 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 wanted a force multiplier, CrowdStrike gives us the ability to be more of a cyber intelligence and cyber fraud team … moving us from cybersecurity to overall security."
— Alex Arango, Deputy CISO, Mercury Financial

CrowdStrike Products

Falcon Cloud Security

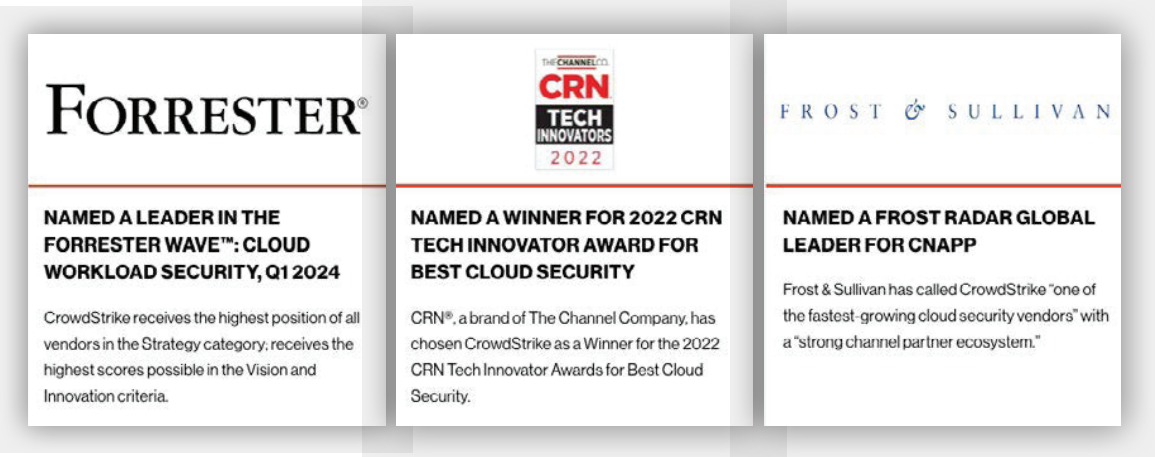
Features	Falcon Cloud Security	Falcon Cloud Security for Containers	Falcon for Managed Containers
Cloud Control Plane			
Cloud security posture management (CSPM)	√	√	X
Behavioral indicators of attack for cloud	√	√	X
Compliance and auditing	√	√	X
Identity analyzer (CIEM)	√	√	X
Infrastructure as code (IaC)	√	√	X
DSPM	√	√	X
Cloud Asset Visibility			
Single unified platform (UI)	√	√	√
Workload Protection			
Cloud workload protection for Windows and Linux (OS)	√	√	X
Runtime protection	√	√	√
Container security	X	√	√
Container image assessment	X	√	√
Agent-based workload protection	√	√	√
Container asset visibility	√	√	√
Agentless workload protection	√	√	X
Drift detection for containers	X	√	√
Kubernetes misconfigurations	X	√	√
Protection for lean OS and serverless containers	X	√	√
Integrations			
AWS	√	√	√
Microsoft Azure	√	√	√
Google Cloud	√	√	√
Red Hat OpenShift	X	√	√
Registry integrations *Please see list on the next page	X	√	√
Licensing			
License	Reserve **OR** On Demand	Reserve **OR** On Demand	On Demand

For a list of full 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 toolset 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	Terraform

Industry Recognition



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/

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/

Request a Cloud Security Health Check