CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Cloud Security

Unify proactive security and cloud runtime protection to prevent breaches, reduce complexity, and secure your hybrid cloud environments

Cloud is the new battleground

As organizations continue to adopt the cloud, it has become the new attack battleground. Adversaries are moving faster than ever. The average breakout time is 48 minutes with the fastest recorded breakout time of just 51 seconds, leaving organizations with little time to detect and respond.[1] This creates mounting challenges for cloud security and security operations teams.

Most organizations attempt to secure the cloud using a patchwork of security and vulnerability management tools, covering different layers like infrastructure, applications, APIs, data, AI, and SaaS. However, these siloed tools lack integration, generate excessive alerts, and provide limited context, making it difficult to prioritize risks effectively. The result? Increased inefficiency, inter-team friction, slow remediation, and a higher risk of breaches.

Meanwhile, adversaries exploit this complexity. Attackers frequently use compromised endpoints and stolen identities to escalate into hybrid cloud environments, exfiltrating sensitive data and disrupting business operations. Security teams need a unified, proactive, and protective approach to outpace modern threats and prevent breaches.

Key benefits

- **Faster Threat Detection and Response:** Achieve up to 89% faster cloud detection and response, reducing attacker dwell time and minimizing breach impact.[2]
- **Improved Cloud Security Visibility:** Gain up to 72% faster ability to monitor the entire cloud estate, enabling proactive risk management.[3]
- **Cost and License Reduction:** Eliminate redundant tools and consolidate security with a unified platform, leading to up to 83% reduction in cloud security licenses and up to $380K in annual savings on average.[3]
- **Operational Efficiency:** Free up security teams with automation and streamlined workflows, saving up to 65 hours per month (equivalent to one FTE per week per month).[3]
- **Stronger Security Posture:** Standardize security across hybrid cloud environments with up to 71% improvement in policy consistency to reduce misconfigurations and security gaps.[3]

[1] CrowdStrike 2025 Global Threat Report

[2] Mercury Financial Builds a Security Ecosystem Around CrowdStrike

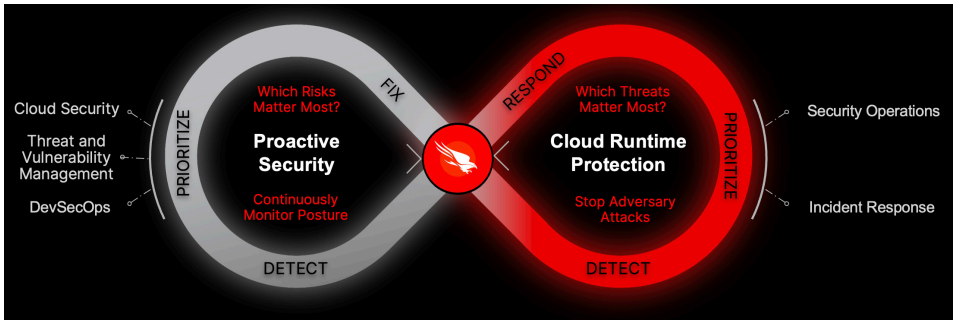
[3] These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.

Stop cloud breaches with CrowdStrike

CrowdStrike Falcon® Cloud Security simplifies this complexity with a unified solution, a single sensor, and uniform policies that seamlessly provide proactive security and cloud runtime protection across on-premises and public clouds:

- **Proactive Security:** Provides unified security posture management (USPM) and business context across cloud layers, leveraging industry-leading threat intelligence, end-to-end attack paths, and ExPRT.AI, CrowdStrike's predictive risk prioritization AI engine. Cloud teams can swiftly prioritize their work, neutralize critical risks, and leave adversaries no room to strike.
- **Cloud Runtime Protection:** Delivers leading cloud runtime workload protection (CWP) and cloud detection and response (CDR), allowing SOC teams to detect and respond to active threats across hybrid clouds so adversaries are stopped in their tracks.

CrowdStrike offers both proactive and protective security as a managed service (MDR) through CrowdStrike Falcon® Adversary OverWatch™ cross-domain threat hunting and CrowdStrike Falcon® Complete Next-Gen MDR, powered by integrated threat intelligence to protect the cloud control plane, host OS, and data plane.



Key capabilities

Proactive Security

- **Agentless Discovery:** Instantly identify and assess cloud assets, misconfigurations, vulnerabilities, and security gaps without deploying an agent.
- **Unified Security Posture:** Continuously monitor cloud risks across cloud security posture management (CSPM), application security posture management (ASPM), data security posture management (DSPM), AI security posture management (AI-SPM), and cloud infrastructure entitlement management (CIEM) to provide full-stack security insights.
- **ExPRT.AI:** Prioritize threats based on reachability, exploitability, and business criticality to focus on what matters most.
- **Adversary Attack Paths:** Map cross-domain attack paths spanning endpoint, identity, and cloud to expose and eliminate potential breach routes.
- **Remediation Steps:** Provide accurate business-context-driven, code-level remediation guidance to accelerate risk mitigation.
- **DevSecOps Workflows:** Integrate security into development pipelines with seamless support for ServiceNow, Jira, Azure DevOps, and GitHub.

Read about CoreWeave, a CrowdStrike customer using Falcon Cloud Security 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

Cloud Runtime Protection

- **Adversary Threat Intelligence:** Detect and stop threats from groups like SCATTERED SPIDER and LABYRINTH CHOLLIMA with real-time intelligence.
- **Industry-Leading Sensor**: Block adversary threats and attacks at runtime with a single, lightweight sensor.
- **Cloud Detection and Response:** Identify and respond to active threats using cloud indicators of attack (IOAs) and attack path analysis.
- **Cloud Workload Protection**: Get real-time coverage across Linux and Windows hosts, containers, Kubernetes, and serverless environments like AWS Fargate.

Falcon Cloud Security licensing

There's a Falcon Cloud Security solution to fit every business:

Proactive Security:

- Unified cloud security posture management including CSPM, DSPM, ASPM, AI-SPM, AI model scanning, CIEM, image and function assessment, infrastructure as code (IaC) scanning, cloud compliance posture insights, and host vulnerability management.

Cloud Runtime Protection:

- **Cloud Runtime Protection:** Breach protection including threat intelligence, CDR, workload runtime protection, and CSPM IOAs across clouds, applications, and data.
- **Cloud Runtime Protection with Containers:** Includes the features and capabilities of Falcon Cloud Security Runtime Protection and adds container and Kubernetes protection. It can be deployed across on-premises, hybrid, and multi-cloud environments.
- **Cloud Runtime Protection with Managed Containers:** Container security and runtime protection for cloud service provider-managed containers, including threat intelligence, CDR, container image security, and Kubernetes protection.

CNAPP:

- Includes the features and capabilities of Proactive Security and Cloud Runtime Protection.

CNAPP with Containers:

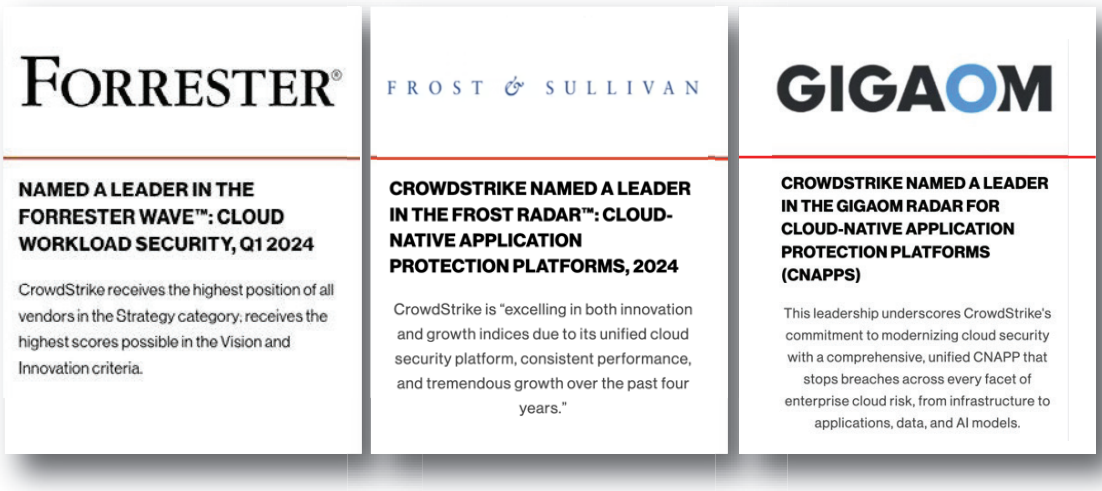
- Includes the features and capabilities of CNAPP and adds container protection.

Managed Services:

- **Falcon Complete Next-Gen MDR:** 24/7 protection for cloud workloads with continuous monitoring, proactive threat hunting, and expert-led response. Powered by the CrowdStrike Falcon® platform, this service delivers real-time defense against advanced cloud threats, enabling organizations to secure cloud environments efficiently — without the cost or complexity of managing security in-house.

Falcon Cloud Security licensing solutions						
Features	**Proactive Security**	**Cloud Runtime Protection**	**Cloud Runtime Protection with Containers**	**Cloud Runtime Protection with Managed Containers**	**CNAPP**	**CNAPP with Containers**
Asset Visibility						
Single unified platform	√	√	√	√	√	√
Cloud asset discovery and inventory	√	√	√	X	√	√
Container asset visibility	√	√	√	√	√	√
Unified Security Posture Management						
Cloud (CSPM)	√	X	X	X	√	√
Attack Path Analysis	√	X	X	X	√	√
Application (ASPM)	√	X	X	X	√	√
Identity (CIEM)	√	X	X	X	√	√
Data (DSPM)	√	X	X	X	√	√
AI (AI-SPM)	√	X	X	X	√	√
IaC scanning	√	X	X	X	√	√
Snapshot agentless security	√	X	X	X	√	√
Cloud compliance	√	X	X	X	√	√
Vulnerability Management						
Host vulnerability management	√	X	X	X	√	√
Container image assessment	√	X	√	√	√	√
ExPRT.AI risk scoring	√	X	√	√	√	√
AI model scanning	√	X	√	√	√	√
Serverless function assessment	√	X	√	√	√	√
16 registry integrations	√	X	√	√	√	√
Cloud Runtime Protection						
CDR (includes cloud IOAs)	X	√	√	X	√	√
CWP for Windows and Linux (OS)	X	√	√	X	√	√
Container runtime protection	X	X	√	√	X	√
Protection for lean OS and serverless containers	X	X	√	√	X	√
Drift detection for containers	X	X	√	√	X	√
Kubernetes misconfigurations	√	X	√	√	√	√
Container compliance	X	X	√	√	X	√

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.