

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 expand their cloud footprint, adversaries follow. Cloud-conscious intrusions by state-nexus threat actors surged 266% in 2025.¹ Attackers are also moving faster than ever, with an average breakout time of 29 minutes in 2025 — and the fastest recorded breakout happened in just 27 seconds.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 \$480K in annual savings on average.³
- **Operational Efficiency:** Free up security teams with automation and streamlined workflows, saving up to 130 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 2026 Global Threat Report

² Mercury Financial Builds a Security Ecosystem Around CrowdStrike. Individual results may vary.

³ The above numbers reflect the median inputs provided by customers during post-sale motions that compare the value of CrowdStrike with incumbent solutions and are not guaranteed. They are intended to demonstrate potential value compared to incumbent solutions and do not represent promised outcomes. Actual value realized will depend on individual customer module deployment and environment.

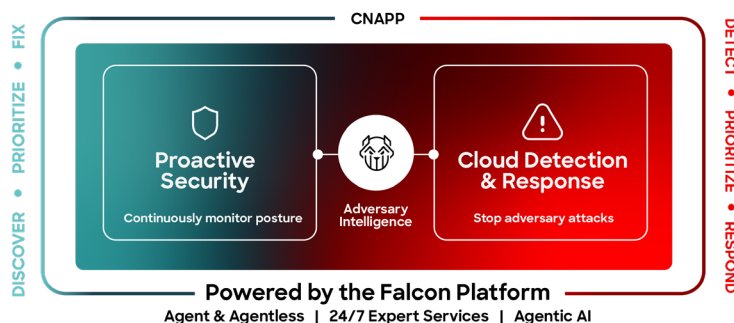
Stop cloud breaches with CrowdStrike

CrowdStrike Falcon® Cloud Security is the cloud-native application protection platform (CNAPP) that stops cloud breaches.

Built for today's hybrid and multi-cloud environments, Falcon Cloud Security protects the entire cloud attack surface — from code to runtime — by combining continuous proactive security with real-time detection and response:

- **Cloud Runtime Protection:** CrowdStrike takes an adversary-first approach to cloud defense, delivering a truly comprehensive hybrid runtime strategy. With a single sensor, augmented by rich agentless telemetry, Falcon Cloud Security delivers industry-leading cloud workload protection (CWP) and real-time cloud detection and response (CDR) to defend against active attacks across hybrid cloud environments. With battle-tested, real-time cloud indicators of attack (IOAs), automated response from the workload to the cloud control plane, and native integrations with identity and endpoint context, defenders are equipped to stop cloud breaches.
- **Proactive Security:** To reduce risk before attacks occur, Falcon Cloud Security delivers agentless-driven posture management that proactively shrinks the cloud attack surface. Unlike typical solutions, CrowdStrike enriches cloud risk detections with adversary intelligence and graph-based context, enabling security teams to prioritize exploitable exposures and prevent breaches before they happen.

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 managed detection and response (MDR), powered by integrated threat intelligence to protect the cloud control plane, host OS, and data plane.



Validated by Third Parties

A Forrester Total Economic Impact™ (TEI) study found the following about Falcon Cloud Security:

264%

ROI over 3 years

<6-month

payback period

\$10M

net present value

The Forrester TEI study also found that Falcon Cloud Security provides:

45% stronger cloud security from enhanced visibility and detection of cloud runtime threats

30% reduction in mean time to detect (MTTD) and mean time to respond (MTTR)

30% reduction in time to identify and prioritize high-risk misconfigurations

[Read the full report](#)

Key capabilities

Proactive Security

- **Agentless Discovery:** Instantly identify and assess cloud assets, misconfigurations, vulnerabilities, and security gaps without disruption to operations.
- **Graph-Based Context:** Correlate assets, identities, configurations, and activity to reveal hidden relationships, attack paths, and risk exposure, backed by graph database technology.
- **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.

- **Adversary Risk Intelligence:** Automatically map cloud risks to real-world adversary groups and their tactics, techniques, and procedures (TTPs), and score vulnerabilities beyond CVSS and EPSS using CrowdStrike ExPRT.AI to prioritize exposures based on CrowdStrike's leading intelligence.
- **Vulnerability Reachability:** Identify reachable vulnerabilities using code-level runtime analysis to prioritize remediation based on exploitability.
- **Adversary Attack Paths:** Map cross-domain attack paths spanning endpoint, identity, and cloud to expose and eliminate potential breach routes.
- **Timeline Explorer:** Connect related cloud changes in a visual timeline to reveal the root cause of risk and replace manual investigation.
- **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.

Cloud Runtime Protection

- **Adversary Threat Intelligence:** Detect and stop threats from groups like SCATTERED SPIDER and LABYRINTH CHOLLIMA with real-time intelligence.
- **Cloud Asset Inventory:** Continuously discover cloud accounts, services, identities, and workloads to give SOC teams a complete, current view of what they are defending.
- **Battle-Tested, Real-Time Cloud IOAs:** Get real-time visibility into malicious events on the cloud control plane.
- **Industry-Leading Sensor:** Get real-time visibility and detections on cloud workloads with a single, lightweight sensor.
- **Falcon Next-Gen SIEM Unified Cases:** Enable seamless cross-domain investigations and workflow creation using natively unified cloud telemetry and detections with identity and endpoint context in CrowdStrike Falcon® Next-Gen SIEM.
- **Real-Time Response:** Help to stop cloud breaches with immediate agent-based and agentless containment of active attacks through CrowdStrike Falcon® Fusion SOAR.

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

"When you're protecting over 100 million members across multiple software platforms and cloud services, it's complicated ... CrowdStrike lets me see everything and how it all interrelates. That saves time, money, and resources for a midsize business with a small team."

– Jesse Webb, CISO and SVP Information Systems, Avalon Healthcare Solutions

"CrowdStrike Falcon Cloud Security extends prevention and detection to containerized workloads, while shared telemetry across modules delivers seamless visibility across every environment."

– Jaifar Al Mamari, CISO, Vodafone Oman

"We can see exactly what services are running in Kubernetes ... If something is malicious, it's blocked immediately by CrowdStrike. 90% of alerts are resolved automatically, so we rarely have to step in."

– Gaurav Verma, Head of IT Risk and Security, Monvia

Falcon Cloud Security licensing

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

Falcon Cloud Security: 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, CrowdStrike Falcon® Spotlight, and CrowdStrike Falcon® Exposure Management

Falcon Cloud Security: Cloud Runtime Protection

- **Cloud Detection and Response:** Breach protection including threat intelligence, agent-based and agentless cloud detections and response, and multi-cloud support
- **Cloud Detection and Response with Containers:** Includes the features and capabilities of Cloud Detection and Response and adds container and Kubernetes protection — can be deployed across on-premises, hybrid, and multi-cloud environments
- **Cloud Detection and Response with Managed Containers:** Container security and runtime protection for cloud service provider-managed containers, including threat intelligence, CDR, container image security, and Kubernetes protection

Falcon Cloud Security: CNAPP

- Includes the features and capabilities of Falcon Cloud Security: Proactive Security and Falcon Cloud Security: Cloud Runtime Protection
- **CNAPP with Containers:** Includes the features and capabilities of CNAPP and adds container protection

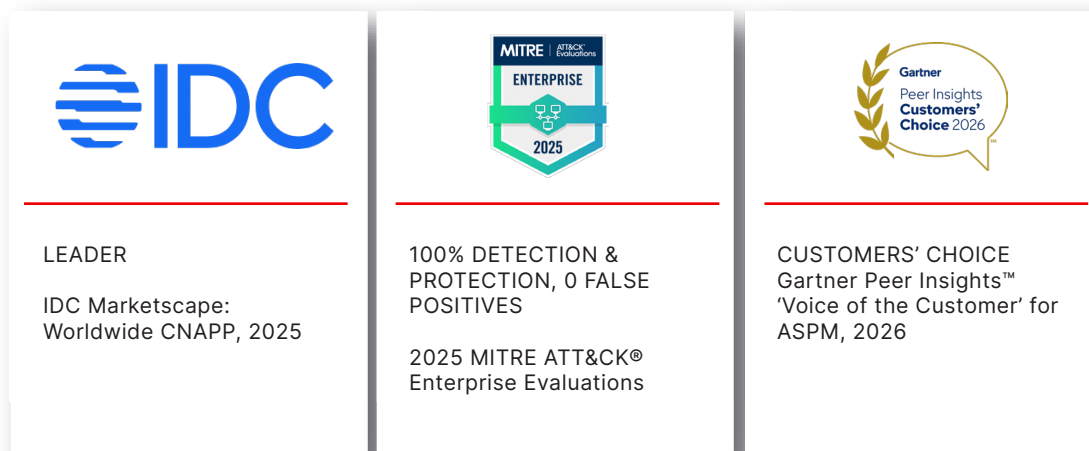
Falcon Complete:

- **Managed Services:** 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 Detection and Response	Cloud Detection and Response with Containers	Cloud Detection and Response with Managed Containers	CNAPP	CNAPP with Containers
Asset Visibility						
Single unified platform	✓	✓	✓	✓	✓	✓
Cloud asset discovery and inventory	✓	✓	✓	✗	✓	✓
Container asset visibility	✓	✗	✓	✓	✓	✓
Graph Explorer	✓	✓	✓	✓	✓	✓
Unified Security Posture Management						
Cloud (CSPM)	✓	✗	✗	✗	✓	✓
Attack Path Analysis	✓	✗	✗	✗	✓	✓
Application (ASPM)	✓	✗	✗	✗	✓	✓
Identity (CIEM)	✓	✗	✗	✗	✓	✓
Data (DSPM)	✓	✗	✗	✗	✓	✓
AI (AI-SPM)	✓	✗	✗	✗	✓	✓
IaC scanning	✓	✗	✗	✗	✓	✓
Agentless vulnerability assessment	✓	✗	✗	✗	✓	✓
Cloud compliance	✓	✗	✗	✗	✓	✓
Exposure management	✓	✗	✗	✗	✓	✓
Vulnerability Management						
Host vulnerability management	✓	✗	✗	✗	✓	✓
Container image assessment	✓	✗	✓	✓	✓	✓
ExPRT.AI risk scoring	✓	✗	✓	✓	✓	✓
AI model scanning	✓	✗	✓	✓	✓	✓
Serverless function assessment	✓	✗	✓	✓	✓	✓
Container registry scanning	✓	✗	✓	✓	✓	✓
Drift detection for containers	✗	✗	✓	✓	✗	✓
Cloud Runtime Protection						
Falcon Next-Gen SIEM*	✓	✓	✓	✓	✓	✓
Real-time cloud detections	✗	✓	✓	✗	✓	✓
Anomaly-based detections	✗	✓	✓	✗	✓	✓
CWP for Windows and Linux (OS)	✗	✓	✓	✗	✓	✓
Kubernetes detections	✗	✗	✓	✗	✗	✓
Protection for lean OS and serverless containers	✗	✗	✓	✓	✗	✓
OOTB cloud-native response playbooks through Falcon Fusion SOAR	✗	✓	✓	✗	✓	✓

*includes Falcon Next-Gen SIEM for telemetry collected by Falcon Cloud Security and other CrowdStrike first-party data

Industry recognition



Forward-Looking Statements

This data sheet may include discussion of unreleased services or features. Any unreleased services or features referenced here are still in development and subject to change. Customers should make their purchase decisions based upon features that are currently available.

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.

