

# Falcon Complete Cloud Security

Providing managed detection and response (MDR) for cloud workloads

## Stop cloud breaches with Falcon Complete Cloud Security

The need for speed and agility in today's digital business requires changes to IT infrastructure, most notably a shift to cloud-native architectures and the adoption of DevOps. This shift has led many businesses to incorporate technologies such as containers, microservices and Kubernetes to improve the efficiency and scalability of development efforts and form the foundation for their nextgeneration infrastructure.

These shifts bring about substantial changes in the attack surface. As a result, adversaries have adapted their tactics, techniques and procedures (TTPs) to capitalize on the chaos. Organizations are faced with some common challenges when managing and monitoring security for cloud workloads:

- **Insufficient skilled staff to reliably act on cloud threats, 24/7, in time to stop a breach.** Security alerts provide critical insights into emerging threats, allowing defenders to respond in the critical early stages before a breach can occur. However, they're only valuable if skilled analysts can review and act on them in time. Today, that time frame has shrunk to hours or minutes.
- **Architecting, deploying and managing security can slow down business transformation.** Finding the right talent and technology, and customizing them to meet the needs of your business, takes time, which is often in short supply. As more organizations look to adopt DevOps practices in order to accelerate growth and innovate faster, they are left with an uncomfortable decision: slow down cloud rollouts to enable security architecture, staffing and processes to catch up, or move forward into the unknown with higher risk of a breach.

## Key benefits

**Stop cloud breaches:** Moving to the cloud brings risk and uncertainties, and requires scarce, skilled staff to manage and keep it secure. Falcon Complete Cloud Security brings you focused expertise to stop threats through continuous vigilance, delivering expert protection 24/7.

**Build faster and more securely in the cloud:** The cloud promises infinite scalability and agility, but deploying and managing your security can introduce DevOps drag. Falcon Complete Cloud Security deploys seamlessly and delivers frictionless protection for the cloud.

**Focus on your business:** Mounting a proper cloud defense takes time and resources, stealing focus from your core mission. Falcon Complete Cloud Security delivers predictable security outcomes at a fraction of the cost.

# Falcon Complete Cloud Security

CrowdStrike Falcon® Complete Cloud Security is the first fully managed cloud workload protection solution, leveraging the power of the CrowdStrike Falcon® platform to deliver 24/7 expert security management, threat hunting, monitoring and response for cloud workloads — and backed by CrowdStrike’s industry-leading Breach Prevention Warranty.

Falcon Complete Cloud Security delivers unparalleled security for cloud workloads by combining CrowdStrike’s leading cloud runtime protection (CRP) and CrowdStrike® Falcon OverWatch™ managed threat hunting, together with the expertise and 24/7 engagement of the CrowdStrike Falcon® Complete managed detection and response (MDR) team. Falcon Complete Cloud Security solves the challenge of implementing and running an effective and mature cloud security program without the difficulty, burden and costs associated with building one internally.

## Key capabilities

### 24/7 expertise to defend the cloud

Falcon Complete Cloud Security is powered by the Falcon Complete MDR team, which arms you with seasoned security professionals who have experience in cloud defense, incident handling and response, forensics, security operations center (SOC) analysis and IT administration. The team has a global footprint, allowing true 24/7 “follow the sun” coverage.

- **Experts in the CrowdStrike Falcon platform:** The team ensures your environment is continuously optimized to combat the latest threats, enable DevOps and achieve the best levels of performance and protection.
- **Experts in incident response:** The team comes to you with multiple years of experience in digital forensics and incident response (DFIR).
- **Experts in threat hunting:** The team’s 24/7 human threat hunting uncovers the faintest trace of malicious activity, in near real time.
- **Experts in threat intelligence:** CrowdStrike’s global threat intelligence team brings critical context to the response process.

### Powered by Falcon Cloud Security

CrowdStrike Falcon® Cloud Security provides comprehensive breach protection for workloads and containers, enabling you to build, run and secure applications with speed and confidence.

- **Multi-cloud:** Falcon provides a single platform to protect AWS, Azure and Google Cloud.
- **Broad visibility:** Uncover AWS EC2 instances, GCP Compute instances and Azure virtual machines (VMs) without installing an agent.
- **Secure hosts and containers:** Falcon runtime protection defends containers against active attacks.

## Breach prevention warranty

CrowdStrike stands strongly behind its breach protection capabilities. Falcon Complete Cloud Security comes with a Breach Prevention Warranty to cover costs should a breach occur within the protected environment. (Breach Prevention Warranty not available in all regions. See the [Breach Prevention Warranty FAQ](#) for other restrictions.)



Falcon Complete Cloud Security

### Continuous human threat hunting

Falcon Complete Cloud Security includes 24/7 threat hunting by the Falcon OverWatch team, CrowdStrike's human threat detection engine that hunts relentlessly to see and stop the most sophisticated hidden threats.

- **The SEARCH methodology:** Falcon OverWatch analysts leverage the proprietary SEARCH methodology to shine a light into the darkest corners — leaving adversaries with nowhere to hide.
- **Cloud-scale data:** Scalable and effective threat hunting requires access to vast amounts of data and the ability to mine that data in real time for signs of intrusions. CrowdStrike's rich telemetry creates the foundation for Falcon OverWatch threat hunting.

### Surgical remediation

When an intrusion is identified in a system protected by the Falcon platform, the Falcon Complete team acts quickly and decisively. The team remotely accesses the affected system using native Falcon capabilities to surgically remove persistence mechanisms, stop active processes and clear other latent artifacts. Falcon Complete restores systems to their preintrusion state without the burden and disruption of reimaging. See the [Falcon Complete FAQ](#) for more details.

- **<60 minutes — average time to perform surgical remediation:** The Falcon Complete team executes surgical remediation remotely in minutes, eliminating the cost and burden of reimaging.
- **Zero impact to DevOps:** The Falcon Complete team can often perform remediation without impacting the underlying applications.

## 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](#) | [Twitter](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

© 2023 CrowdStrike, Inc.  
All rights reserved.



[Schedule a Demo](#)

Learn more at [www.crowdstrike.com](http://www.crowdstrike.com)