

# Falcon Complete GovCloud



Managed detection and response (MDR) to secure all public sector critical areas of risk and sensitive data

## Challenges

Securing U.S. public sector organizations is a monumental task, especially in today's complex threat environment. Adversaries are faster, stealthier and capable of achieving lateral movement in minutes.

With growing attack surfaces and hybrid workforces, it has become more critical than ever for organizations to streamline security operations and protect critical areas of risk in order to maintain a proactive stance against sophisticated and motivated adversaries.

## Solution

CrowdStrike Falcon® Complete GovCloud MDR delivers 24/7 expert management, monitoring and response for the CrowdStrike Falcon® platform for the public sector. With comprehensive, specialized threat detection, threat hunting, investigation and full-cycle remediation, public organizations gain a team of elite experts that act as a force multiplier for IT and security teams — ensuring comprehensive protection across key attack surfaces.

CrowdStrike strongly supports the mission of civilian government, the military and the intelligence community to deliver advanced services with protection designated at Impact Level 5 (IL5) Provisional Authorization (PA) by the United States Department of Defense (DoD). The Falcon Complete GovCloud team is tailored for securing the U.S. public sector and authorized to operate by the DoD Cloud Computing Security Requirements Guide (CC SRG) to cover Controlled Unclassified Information (CUI) and National Security Systems (NSS) Data.

The CrowdStrike Falcon® platform is hosted on AWS GovCloud and is Federal Risk and Authorization Management Program (FedRAMP)-authorized, providing government agencies the complete protection and visibility they need to mitigate risk and eliminate threats on federal, state and local levels.

## Key benefits

24/7 managed security operations

Prioritized, actionable detections and security insights

Comprehensive threat visibility across the security stack

Advanced protection with proactive threat hunting and native threat intelligence

FedRAMP High and DoD CC SRG IL5 Compliance

## Key capabilities

### Layers of Expertise

The Falcon Complete GovCloud team is composed of seasoned security professionals with experience in incident handling, incident response, forensics, security operations center (SOC) analysis, identity protection and IT administration.

**Experts in the CrowdStrike Falcon platform:** The Falcon Complete GovCloud team holds CrowdStrike Certified Falcon Responder (CCFR) and CrowdStrike Certified Falcon Administrator (CCFA) certifications.

**Experts in incident response:** The Falcon Complete team has years of experience in digital forensics and incident response (DFIR).

**Experts in threat hunting and threat intelligence:** The CrowdStrike® Falcon OverWatch™ threat hunting team and CrowdStrike's AI-driven intelligence built into the Falcon platform deliver integrated insights to strengthen defenses and disrupt attacks before they can turn into breaches.

**U.S.-based:** The Falcon Complete GovCloud team is 100% U.S.-based.

**Detection across endpoints, cloud workloads and identities:** Falcon Complete enables frictionless endpoint, cloud workload and identity security, delivering comprehensive protection to outpace the adversary.

### Transparent and Secure Collaboration

**Message Center:** This secure bi-directional communication channel allows for information exchange about emerging incidents as well as ad hoc questions, all directly within the Falcon console. Keeping communications close to the Falcon data provides maximum efficiency, ensuring the full context associated with emerging threats is readily available.

**Executive dashboards:** Gain at-a-glance visibility into the day-to-day activity that Falcon Complete performs, including trends and actionable insights.

**Message analyst:** Fast access to CrowdStrike experts is embedded throughout the Falcon console. This helps analysts more quickly understand threats and get fast answers to their cybersecurity questions.

### Full-Cycle Remediation

When an intrusion is identified, the Falcon Complete GovCloud team acts quickly and decisively, remotely accessing the affected system using native Falcon capabilities to surgically remove persistence mechanisms, stop active processes, disrupt identity-based threats and clear other latent artifacts.

The Falcon Complete GovCloud team has the ability to restore systems to their pre-intrusion state without the burden and disruption of reimaging systems.

### CrowdStrike Compliance and Certification

CrowdStrike can help you meet your compliance and regulatory needs with certifications across:

- Payment Card Industry Data Security Standard (PCI DSS)
- Cybersecurity Maturity Model Certification (CMMC)
- **FedRAMP:** As of September 2018, CrowdStrike Falcon® on GovCloud is recognized as "FedRAMP Authorized" on the FedRAMP Marketplace
- Provisional Authorization to Operate (P-ATO) at Impact Level 4 (IL4) granted in April 2022, through the Defense Information Systems Agency (DISA) Cloud Computing Security Requirements Guidance (CC SRG). CrowdStrike Falcon on GovCloud was granted P-ATO at Impact Level 5 (IL5) in May 2023.



## What Falcon Complete customers say

"By analyzing the millions of data points generated by a vast and diverse customer base, often in real time, CrowdStrike is able to provide our team with a comprehensive and clear picture of exactly what is happening across the globe, 24/7. That's an essential ingredient in protecting us from issues long before they become a problem."

**Michael Taylor**, IT Director, Mercedes-AMG Petronas Formula One Team

"Falcon Complete provides operational efficiencies and augments our in-house security operations with 24/7 coverage, responsiveness and a level of visibility we didn't have before."

**Thierry Delaitre**, Head of IT Developments, Information Systems and Support, University of Westminster

- Defense Information Systems Agency (DISA)
- Criminal Justice Information Services (CJIS)
- Health Insurance Portability and Accountability Act (HIPAA)
- National Institute of Standards and Technology (NIST)
- Federal Financial Institutions Examination Council (FFIEC)
- National Security Agency Cyber Incident Response Assistance (NSA-CIRA), SOC 2®
- AV Comparatives testing
- Cloud Security Alliance (CSA) security
- Security Trust Assurance and Risk (STAR) attestation
- Anti-Malware Testing Standards Organization (AMTSO)
- Voluntary Product Accessibility Template (VPAT)
- General Data Protection Regulation (GDPR)
- [And more](#)

# CrowdStrike's Breach Prevention Warranty

**Rest assured with the most comprehensive Breach Prevention Warranty\***

Rest assured with an industry-leading, comprehensive breach prevention warranty. CrowdStrike stands strongly behind its breach protection capabilities — Falcon Complete comes with a Breach Prevention Warranty to cover costs in the event a breach occurs within the protected environment.



	Other Warranties	CrowdStrike
Time to report requirements	24-48 hours	72 hours
Categories covered	Limited	✓
Backed by the largest insurance providers	Varies	✓
Primary coverage	Varies	✓
Policy requirements	Extensive	Minimal

\*Learn more in the [Breach Prevention Warranty FAQ](#).

## 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.

