

Falcon Complete Next-Gen MDR on GovCloud

Next-gen managed detection and response (MDR) to
secure all critical areas of risk

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

CrowdStrike strongly supports the mission of civilian government, the military and the intelligence community and delivers advanced next-gen MDR services with protection designated at Impact Level 2 (IL2) by the U.S. Department of Defense (DoD).

The CrowdStrike Falcon® platform is hosted on AWS GovCloud and is Federal Risk and Authorization Management Program (FedRAMP) High, providing government agencies the protection and visibility they need to mitigate risk and eliminate threats at the 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 IL2 Compliant

Key capabilities

Layers of Expertise

Falcon Complete Next-Gen MDR has a dedicated GovCloud team 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 Next-Gen MDR GovCloud team holds CrowdStrike Certified Falcon Responder (CCFR) and CrowdStrike Certified Falcon Administrator (CCFA) certifications.
- **Experts in incident response:** The Falcon Complete Next-Gen MDR GovCloud team has years of experience in digital forensics and incident response (DFIR).
- **Experts in threat hunting and threat intelligence:** CrowdStrike Counter Adversary Operations, powered by the CrowdStrike® Falcon Adversary OverWatch™ threat hunting team and the CrowdStrike Intelligence team, sees and stops undetected, sophisticated threats while bringing critical context to the response process.
- **U.S.-based:** The Falcon Complete Next-Gen MDR GovCloud team is 100% U.S.-based.

Breaches Stopped Across the Attack Surface

- **Get proactive endpoint protection:** Falcon Complete Next-Gen MDR leverages CrowdStrike Falcon® Insight XDR detection and response for endpoint and beyond, CrowdStrike Falcon® Prevent next-gen antivirus and CrowdStrike Falcon® Discover IT hygiene to stop threats targeting your endpoints 24/7, stepping in to kill malicious processes, quarantine files and remove persistence.
- **Stop identity-based attacks:** Leveraging CrowdStrike Falcon® Identity Protection, Falcon Complete Next-Gen MDR can stop identity-based attacks in their tracks, with real-time identity threat prevention and IT policy enforcement.
- **Secure cloud workloads:** With CrowdStrike Falcon® Cloud Security, Falcon Complete Next-Gen MDR uncovers and eradicates cloud intrusions in real time, delivering comprehensive managed protection for cloud workloads and containers.
- **Extend protection to critical data sources:** With unified threat data from CrowdStrike Falcon® Next-Gen SIEM, Falcon Complete Next-Gen MDR expands the scope of visibility and protection beyond native Falcon telemetry to accelerate threat investigation and eradicate threats earlier in the kill chain.

Third-party domains include:

- Email security
- Web security/cloud access security broker (CASB)
- Network detection and response (NDR)
- Remote access solutions (VPN)
- Identity and access management (IAM)
- And more

What Falcon Complete customers say

"CrowdStrike is there for us 24/7/365 and gives more flexibility for my team to take time off, as the company really has our back. It's like having a secondary SOC, and indeed many times functions as our primary operations center for endpoints."

Shannon Lawson, CISO, City of Phoenix

"The constant presence of the Falcon Complete team is like having a 24/7 security operations center. For us to replicate that would require hiring 6-10 employees, plus dealing with all the challenges of fielding such a high-performance team."

Jason Strohbehn, Deputy CISO, State of Wyoming

CrowdStrike Products

Falcon Complete Next-Gen MDR on GovCloud

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 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 Next-Gen MDR 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 Next-Gen MDR 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 Next-Gen MDR 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 the following:

- Payment Card Industry Data Security Standard (PCI DSS)
- Cybersecurity Maturity Model Certification (CMMC)
- **FedRAMP:** CrowdStrike Falcon® on GovCloud is FedRAMP High authorized on the FedRAMP Marketplace.
- 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 and Security Trust Assurance and Risk (STAR) attestation
- 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.*

CrowdStrike stands strongly behind its breach protection capabilities — Falcon Complete Next-Gen MDR 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.

CrowdStrike: We stop breaches.



Schedule a Demo