CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Complete for State and Local Government

Managed detection and response (MDR) to defend citizen data and services against cyberattacks

Challenge

Adversaries thrive in blind spots, and unfortunately, state and local governments have been known to have their fair share. As government IT leaders deal with budget constraints, lack of cybersecurity expertise and the overwhelming task of securing complex environments, adversaries have only become more relentless and destructive in their attacks.

When combating advanced threats, every minute counts. Even with the right point products, effective threat detection and response requires more than technology. The right expertise, process and strategy are equally crucial in ensuring cybersecurity efforts operate efficiently 24/7 and avoiding costly business disruption.

Solution

CrowdStrike Falcon® Complete MDR is a cutting-edge cybersecurity service designed to meet the unique challenges state and local governments face in securing their infrastructure. With advanced threat detection capabilities, comprehensive endpoint protection and centralized management, Falcon Complete enables state and local governments to adopt a holistic approach to cybersecurity. This data sheet outlines the key benefits of Falcon Complete and how it empowers governments to extend support to local counties, cities, municipalities and school systems across the state.

Key Benefits

- 24/7 managed security operations
- Prioritized, actionable detections and security insights with minimal downtime
- Comprehensive threat visibility across the security stack
- Advanced protection with proactive threat hunting and native threat intelligence
- Rapid response actions against sophisticated attacks, enriched with first- and third-party telemetry

Key capabilities

Comprehensive endpoint protection

Falcon Complete provides state-of-the-art endpoint protection, securing all devices across state or local government networks. Its next-generation antivirus (NGAV) engine combines artificial intelligence-driven threat detection, machine learning algorithms and behavioral analytics to proactively identify and block known and unknown threats. This ensures government systems and data remain protected against advanced malware, ransomware and other sophisticated cyberattacks.

Advanced threat detection and response

Falcon Complete leverages the power of cloud-native architecture, CrowdStrike Threat Graph® and a vast intelligence network to provide real-time threat detection and response capabilities. Through continuous monitoring and analysis, Falcon Complete provides 24/7 expert-driven management, threat hunting, monitoring, investigation and response across the attack surface to stop breaches. This empowers state and local governments to proactively defend against targeted attacks, advanced persistent threats (APTs) and emerging threats, reducing the risk of data breaches and system compromises — all without lifting a finger, performed entirely by the Falcon Complete team.

Centralized management and visibility

Falcon Complete offers a centralized management platform that enables state and local governments to streamline their cybersecurity operations. The CrowdStrike Falcon® console provides a single-pane-of-glass view into the entire network's security posture, allowing Falcon Complete to efficiently manage and monitor endpoints, investigate incidents and enforce security policies across various entities. This centralized approach enhances visibility, simplifies compliance reporting and enables proactive incident response. Falcon Complete offers customers implementation, platform management, and response and remediation services for advanced threats without the burden, overhead or costs of deploying and managing a 24/7 threat detection and response function on their own.

Extensibility and scalability

Falcon Complete is designed to support the unique needs of state governments, including the ability to extend protection to local counties, cities, municipalities and school systems. The solution allows for easy deployment, management and scaling across multiple entities, ensuring consistent security standards throughout the government infrastructure. This collaborative approach strengthens overall cybersecurity resilience and promotes information sharing among government entities.

CrowdStrike Falcon Complete supports the following:

- CrowdStrike Falcon® Prevent
- CrowdStrike Falcon® Insight XDR
- CrowdStrike Falcon® Device Control
- CrowdStrike Falcon® Discover
- CrowdStrike Falcon® Identity Threat Protection
- CrowdStrike Falcon® Cloud Security (managed cloud workload protection only)
- CrowdStrike Falcon® Intelligence
- CrowdStrike® Falcon OverWatch™

Real-time identity threat protection

Minutes matter when an attack occurs, and your defenders may be hours away from their keyboards. Falcon Complete executes surgical remediation to stop identity-driven attack techniques in their tracks at any time of the day or night.

- Enforcement of multifactor authentication (MFA): When suspicious activity is identified, Falcon Complete analysts can trigger reauthentication with MFA, shutting the door on intruders.
- Reset of compromised passwords: An adversary with valid credentials is free to return again and again and move at will across the network. Falcon Complete takes decisive action to revoke unauthorized access at the source.
- Surgical remediation in minutes: The Falcon Complete team executes remediation remotely in near real time, eliminating the cost and burden of reimaging.

Rapid incident response and remediation

In the event of a security incident, Falcon Complete enables state and local governments to respond swiftly and effectively. With its integrated threat intelligence, automated containment capabilities and forensic analysis, the service team identifies the root cause of an incident, contains the threat and remediates affected systems rapidly. This minimizes downtime, reduces the impact of attacks and helps state and local governments maintain critical services uninterrupted.

24/7 managed detection and response

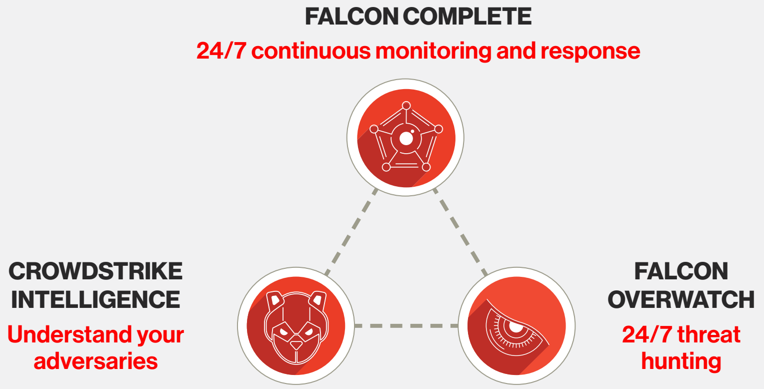
Falcon Complete includes 24/7 access to CrowdStrike's dedicated team of experts, the CrowdStrike Falcon OverWatch threat hunting team. This team of experienced cybersecurity professionals provides continuous monitoring, threat hunting and surgical, proactive response to potential threats, augmenting the state or local government's security capabilities. Their expertise and round-the-clock support enhance incident response readiness and reduce the time to detect and respond to emerging threats.

CrowdStrike Falcon Complete offers governments a comprehensive and extensible cybersecurity solution, empowering them to adopt a whole-of-state approach to security. Through advanced threat detection, centralized management and scalable architecture, Falcon Complete enables state and local governments to protect their infrastructure while extending support to local entities. With Falcon Complete, state and local governments can enhance their cybersecurity resilience, improve incident response capabilities, and safeguard critical systems and data across the entire infrastructure.

79 minutes was the average eCrime breakout time observed.

Source: CrowdStrike 2023 Threat Hunting Report

Effective monitoring and response



FALCON COMPLETE
24/7 continuous monitoring and response

CROWDSTRIKE INTELLIGENCE
Understand your adversaries

FALCON OVERWATCH
24/7 threat hunting

	Industry average*	Continuous monitoring and response
Time to detect	120 hours	**1 minute**
Time to investigate	11 hours	**6 minutes**
Time to remediate	31 hours	**29 minutes**

* Source: CrowdStrike 2020 Global Security Attitude Survey

FALCON COMPLETE EXCEEDS THE 1:10:60 GOAL

Follow us:

- **Blog ›**
- **Twitter ›**
- **LinkedIn ›**
- **Facebook ›**
- **Instagram ›**

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.

Learn more →

Start a free trial today →