CROWDSTRIKE

FALCON COMPLETE NEXT-GEN MDR

IN RESPONSE TO:

G-Cloud 15 Framework (Lots 1-3)

Service Description

150 206 E. 9th Street, Suite 1400, Austin, Texas 78701
TEL: (888)512-8906 | FAX:(949) 417-1289
www.crowdstrike.com

DOCUMENT CONTROL

Date	01/2026

CROWDSTRIKE CONTACT

Account Manager	Peter Carthew Regional Sales Director ukpublicsector@crowdstrike.com

LEGAL DISCLAIMER

CrowdStrike's solution, pricing and offer to provide services and products in this response is expressly conditioned on: (i) CrowdStrike's current understanding of the scope of the project based on the information in the RFI, RFP, RFQ, Security Questionnaires and otherwise available and provided to CrowdStrike; and (ii) the parties negotiating mutually agreeable final terms and conditions upon award.

The information contained in this Response marked "confidential" is considered by CrowdStrike to be proprietary and confidential to CrowdStrike. The information contained in this Response may be used solely in connection with the evaluation of the Response. To the extent that a claim is made under applicable law to disclose confidential information contained in this Response, CrowdStrike reserves the right to defend its confidential information against such claim. Subject to applicable law, you agree (a) to keep the information contained in this Response in strict confidence and not to disclose it to any third party without CrowdStrike's prior written consent and (b) your internal disclosure of the information contained in this Response shall be only to those employees, contractors or agents having a need to know such information in connection with the evaluation of the Response and only insofar as such persons are bound by a nondisclosure agreement consistent with the foregoing. You do not acquire any intellectual property rights in CrowdStrike's property under the Response and you agree to comply with all applicable export control laws and regulations to ensure that no confidential information is used or exported in violation of such laws and regulations. You may make a reasonable number of copies of this Response for your internal distribution for use solely in connection with the evaluation of the Response; otherwise, you may not reproduce or transmit any part of this Response in any form or by any means without the express written consent of CrowdStrike. By reading the Response, you have agreed to be bound by the foregoing terms

INTRODUCTION

COMPANY OVERVIEW

CrowdStrike is a leader in cloud-delivered, next-generation endpoint and cloud workload protection. CrowdStrike has revolutionized endpoint and workload protection by being the first company to unify NGAV, EDR and a 24/7 managed threat hunting service — all delivered through a single lightweight, intelligent agent. CrowdStrike is the pioneer of the first security cloud, which provides comprehensive visibility and protection at scale for every endpoint and workload. Powered by the proprietary CrowdStrike Threat Graph, the CrowdStrike Security Cloud within the Falcon platform regularly correlates trillions of endpoint-related events per week in real time across the globe.

The CrowdStrike Falcon platform provides robust threat prevention, leveraging AI and ML with advanced detection and response and integrated threat intelligence to protect against the modern threat landscape. The Falcon platform offers the following:

- Complete protection from malware and malware-free attacks
- Unrivalled visibility to discover and investigate current and historic endpoint activities
- Ease-of-use

Many of the world's largest organizations already put their trust in CrowdStrike, including 254 of Fortune 500, 526 of Global 2000, 15 of the Top 20 Global Banks, 5 of the Top 10 Largest Healthcare Providers and 7 of the Top 10 Largest Energy Institutions.

In June 2019, CrowdStrike conducted one of the most successful technology initial public offerings (IPOs), listing on Nasdaq.

OVERVIEW OF THE G-CLOUD SERVICE

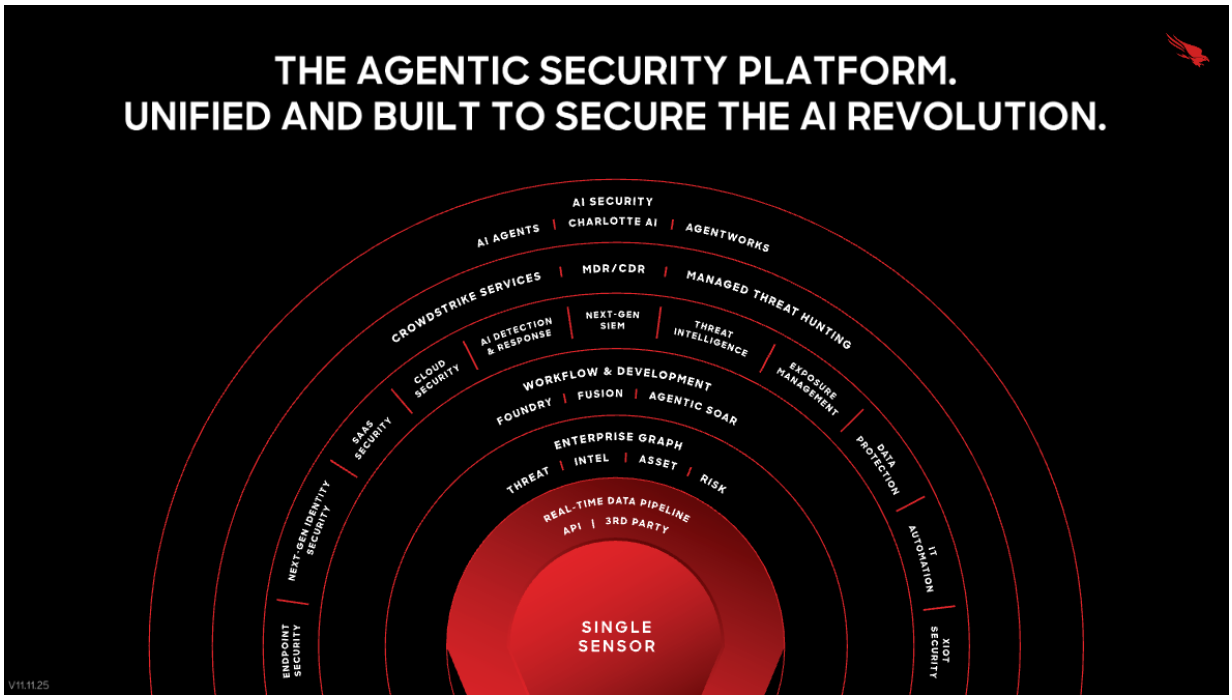
PLATFORM OVERVIEW

Streamlined, single agent architecture
CrowdStrike's single agent is built on a scalable cloud-native platform that's easy to deploy and manage. Say goodbye to managing multiple cybersecurity products with one, unified solution.

Infused with AI expertise
At CrowdStrike, AI is more than a feature — it's in our DNA. With models trained on trillions of data points every day, we predict and stop threats in their tracks.

Effortless workflows and automation
The power of native automation and generative AI workflows is woven into every corner of our platform. We do the heavy lifting, so you can act swiftly and confidently.

Powered by the CrowdStrike® Security Cloud and world-class AI, the 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.



FALCON COMPLETE NEXT-GEN MDR: MANAGED DETECTION AND RESPONSE

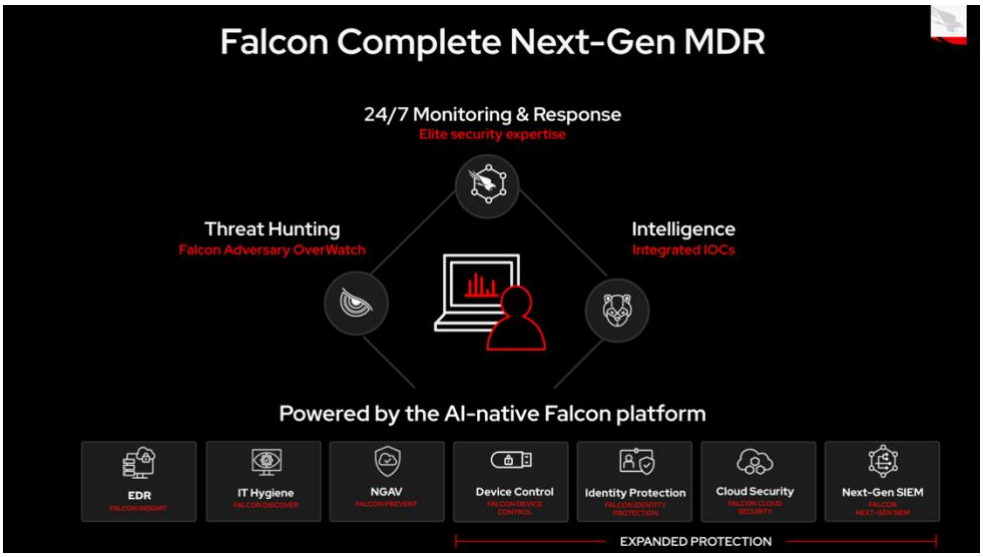
CUSTOMER PROBLEM:

Today's security teams face sophisticated threats and adversaries capable of achieving lateral movement in just 2 minutes and 7 seconds. To keep up with the pace of modern threats and stop breaches, organizations need the right combination of advanced cybersecurity expertise and cutting-edge technology to deliver rapid threat detection, investigation and full-cycle response across all key attack surfaces. Without the right MDR solution, organizations risk falling behind against increasingly sophisticated threats.

WHAT'S NEEDED:

The rise of sophisticated adversaries who can attack anytime and anywhere requires a proactive approach to 24/7 threat detection and response. Organizations should look to MDR for around-the-clock expert-led threat detection, response and hands-on platform management to fortify their defenses against today's fast-moving threats and increase security efficiency. Organizations need MDR to:

- **Augment internal defenses.** Cybersecurity is not just a technology problem — it also requires around-the-clock expertise. MDR delivers focused expertise to stop threats through continuous vigilance and hands-on platform management.
- **Eradicate threats fast.** Adversaries are capable of inflicting damage in minutes, but it can take hours or days for organizations to respond. MDR accelerates security operations, leveraging powerful technology and full enterprise visibility to stop breaches through rapid detection and response.
- **Eliminate risks and save money.** Defending against today's threats is a continuous challenge. Security teams must always wonder, "Am I doing enough?" MDR delivers predictable results and always-on protection at a fraction of the cost of building an in-house SOC.



UNIQUE APPROACH:

CrowdStrike Falcon Complete Next-Gen MDR delivers world-class 24/7 MDR expertise powered by the AI-native Falcon platform. Operating as a seamless extension of customer teams, Falcon Complete Next-Gen MDR delivers advanced threat detection, investigation and response across all key attack surfaces — including endpoint, cloud, identity and critical third-party data — with specialized and proactive threat hunting to accelerate MTTR, close the cybersecurity skills gap and stop breaches.

- **Force multiplier for your team:** Fortify your defenses with 24/7 protection from top security experts. Falcon Complete Next-Gen MDR delivers the expertise needed to close the skills gap and combat today's most advanced threats, including ransomware, phishing attacks and zero-day exploits.
- **Accelerated defense along every point of attack:** Leveraging unified threat data, expanded visibility and cutting-edge generative AI from the Falcon platform, Falcon Complete Next-Gen MDR delivers rapid MTTD.
- **Intelligence-driven threat hunting:** Disrupt sophisticated adversaries with CrowdStrike Falcon Adversary OverWatch, which delivers 24/7 protection across endpoints, identities and cloud workloads using advanced AI, industry-leading threat intelligence and elite human expertise.
- **Full-cycle remediation:** When an intrusion is identified, the Falcon Complete Next-Gen MDR team acts quickly and decisively, remotely accessing affected systems using native Falcon platform capabilities to surgically remove persistence mechanisms, stop active processes and clear other latent artifacts.

Full enterprise visibility and protection:

Falcon Complete Next-Gen MDR delivers comprehensive MDR for endpoints, identities, cloud workloads and critical third-party data through the following:

- **Falcon Discover.** For IT hygiene and comprehensive asset inventory.
- **Falcon Prevent.** Next-gen antivirus with machine learning, exploit blocking, indicators of attack, behavioral analysis and more.
- **Falcon Insight XDR.** Stops threats targeting your endpoints, stepping in to kill malicious processes, quarantine files and remove persistence.

Falcon Complete Next-Gen MDR includes services from:

- **The Falcon Complete Next-Gen MDR team.** 24/7 management, monitoring, response and full-cycle remediation
- **Falcon Adversary OverWatch.** 24/7 human threat hunting across endpoints, identities and cloud workloads

Optional add-on for expanded protection:

- **Falcon Device Control.** Provides the visibility and granular control necessary to limit risks associated with USB devices.
- **Falcon Identity Protection.** Actively monitors and responds to identity-based attacks in real time.
- **Falcon Cloud Security.** Advanced protection of cloud workloads, containers and Kubernetes through expert management.
- **Falcon Next-Gen SIEM.** With unified threat data from Falcon Next-Gen SIEM, Falcon Complete Next-Gen MDR expands the scope of visibility and protection beyond native Falcon telemetry to accelerate threat investigation with critical third-party data to 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

OUTCOME DELIVERED:

Falcon Complete Next-Gen MDR enables organizations to fortify their defenses and stop breaches, backed by CrowdStrike's elite team of security experts.

- **75% reduction in MTTR[1],** dramatically accelerating key SOC processes and improving internal operational efficiencies.
- **4-minute MTTD** to counter the speed and sophistication of adversaries.[2]
- **90% improvement in detection coverage**[12] and enormous visibility improvements driven by the Falcon Complete Next-Gen MDR team, which reviews, triages and resolves Falcon platform detections (low/medium/high/critical severity) on behalf of customers.
- **Helped avoid a headcount increase of 10-12 employees** [3]by outsourcing security to Falcon Complete Next-Gen MDR.

Product Page: https://www.crowdstrike.com/services/falcon-complete-next-gen-mdr/

[1] CrowdStrike Business Value Assessments (BVAs) conducted in partnership with individual Falcon Complete Next-Gen MDR customers

[2] MITRE Engenuity ATT&CK Evaluations: Managed Services, Round 2, menuPass + ALPHV BlackCat (2024)

[3] Business value realized from a customer case study.

DATA PROTECTION

INFORMATION ASSURANCE

CrowdStrike has obtained several compliance certifications that position the company at the top of the security vendor space. These include both ISO27001:2022 and SOC2 Type II. A summary/breakdown and certificates can be provided upon request. For a full breakdown please visit: https://www.crowdstrike.com/why-crowdstrike/crowdstrike-compliance-certification/

DATA BACKUP AND RESTORATION

The offering from CrowdStrike is a SaaS platform and hence localised backups are all covered as part of the native service offering. All information needed about data management is outlined in the Business Continuity section of this Service Definition.

If the customer wishes they can also retrieve all data from within the platform and store it at an alternative location, this data can be retrieved in near real time or weekly in bulk. Several API's exist that allow data to be extracted more surgically for backup or other purposes.

BUSINESS CONTINUITY

CrowdStrike has a documented Business Continuity Plan (BCP). The plan covers every aspect of restoring and recovering the service given a catastrophic data centre failure as well as protecting the confidentiality and integrity of the data. Disaster recovery provisions are included within our BCP.
CrowdStrike hosts the Falcon platform across multiple discrete and redundant data centre's; each data centre has its own power, networking and connectivity, and is housed in separate facilities. High speed, low-latency networks between data centre's support near real-time replication of data, and transparent fail-over in the event of a single data centre outage. The entire process is seamless and transparent to customers.
A summary of the BCP plan elements can be shared with the customer upon request.

PRIVACY BY DESIGN

The CrowdStrike Falcon Platform was designed not only with privacy in mind but as a platform to protect organizations data. Additionally, cybersecurity plays a key role in data protection and GDPR compliance. CrowdStrike's next-generation product offerings, professional services, and global expertise can help organizations meet their GDPR obligations.

CrowdStrike understands that organizations must consider regulatory requirements when choosing vendors. That is why CrowdStrike helps customers enhance their cybersecurity and data protection posture while meeting a wide range of compliance needs. Choosing CrowdStrike as a vendor can be a critical component for helping fulfil GDPR compliance.

- Proudly protects many of the world's largest organisations
- Participates in and has certified its compliance with the EU-U.S. Data Privacy Framework to ensure the adequacy of cross-border transfers
- Meets TRUSTe's Privacy Certification requirements
- We abide by the EU's General Data Protection Regulation (GDPR), and as a data processor,

we provide our customers with a GDPR compliant data processing addendum, which we will need to incorporate in the Call Off Contract. In particular, CrowdStrike Products are hosted on a data centre located in the EU. CrowdStrike's Affiliates worldwide, and its Sub processors, may remotely access Buyer's Data for the purposes described in Exhibit A to the CrowdStrike Terms and Conditions and the CrowdStrike Data Protection Addendum. CrowdStrike Products also leverage a crowdsourcing model for certain customer data to improve its offerings for the benefit of all customers, as described fully at the CrowdStrike Terms and Conditions, Exhibit A, Section 2. CrowdStrike is available to answer any customer questions about this and to ensure this is accurately described in any Call Off Contract.
Please contact CrowdStrike if you require further information.