CROWDSTRIKE

CROWDSTRIKE SERVICES

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

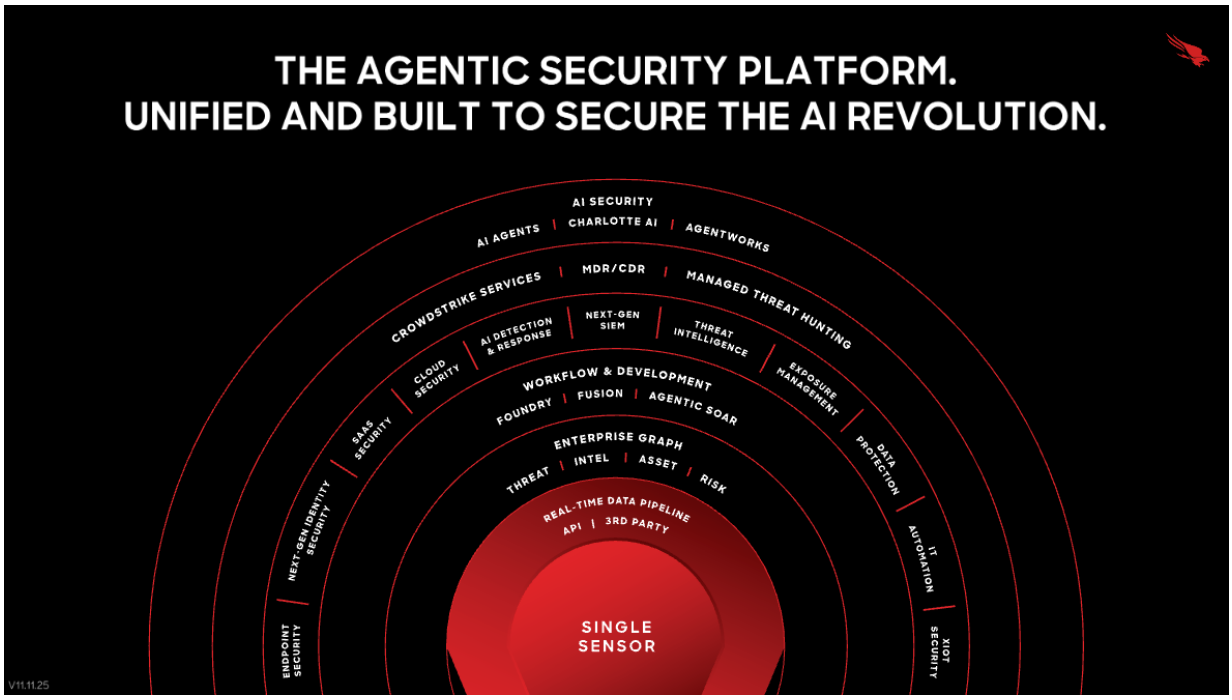
PLATFORM OVERVIEW

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.



CROWDSTRIKE PROFESSIONAL SERVICES

CUSTOMER PROBLEM

Adversaries are more sophisticated than ever before, and a data breach constitutes a severe moment of crisis for victim organizations. Attackers continually find new attack paths to enter environments and then combine seemingly unrelated exploits to create a full-scale data breach or successful ransomware attack. They have advanced tools, networks to support their operations, and the luxury of targeting the weakest entry point at a time of their choosing. The attack surface is sprawling with many entry points for potential adversaries, and underprepared organizations are easy targets for an advanced attack. Many security teams face this uphill battle without proper resources, and may not have adequate tooling for visibility, prevention, detection and response in-house. Teams are often smaller than ideal as organizations struggle to recruit and retain top DFIR talent necessary to defend against threat actors.

When breached, the impacted organization faces business interruption, lost revenue, brand damage, recovery costs and possible regulatory penalties before returning to normal operations. With the average data breach cost in the millions of dollars, and with some ransom demands topping $100M, organizations want to avoid a breach at all costs, or if already compromised, end the breach without delay and minimize the impact.

WHAT'S NEEDED

Avoiding a breach requires that organizations mature their people, processes and technology to a state that is out of reach of the adversaries. Security services that test and validate the security program, processes and decision making are ideal to gain experience and insights that will be crucial to avoiding or mitigating a breach in the future. The worst time to learn a valuable IR lesson is in the midst of a crisis, ideally this experience is gained in advance through simulations, assessments and hands-on exercises.

If a breach occurs, speed and efficiency are the top priorities for the impacted organization. The decisions made during an incident will have the greatest impact on the overall resolution of the incident, meaning that an informed, experienced and highly capable IR partner is essential to saving time, money and brand reputation.

UNIQUE APPROACH

CrowdStrike is the IR provider of choice and de-facto market leader due to our security excellence, unparalleled understanding of adversary tradecraft, and our track record of successful response to the most consequential breaches of the last decade. We've seen it all and we are prepared for anything. The breadth and depth of CrowdStrike's cumulative IR experience from the frontlines of the most impactful cyber breaches of the last decade means that our customers are never outclassed by a sophisticated adversary. When the worst happens and a cyber breach occurs, confidently rely on the best team in the industry to rapidly remediate, recover endpoints, restore systems and guide the recovery process. This IR expertise also propels top-tier outcomes through CrowdStrike Cybersecurity Consulting Services to fortify against a breach, and test a team's preparedness and ability to respond to a sophisticated threat.

Powered by the AI-native CrowdStrike Falcon platform and its innate advantages, including speed to deployment, reduced complexity, industry leading threat intelligence, and our all-encompassing ability to respond to and remediate complex breaches - CrowdStrike Services are the most efficient and effective option to achieve customer-required outcomes.

CROWDSTRIKE PROFESSIONAL SERVICES OFFERINGS INCLUDE:

INCIDENT RESPONSE

24/7 elite incident response to contain threats, restore order and mitigate breach impact

Incident Response | Comprehensive response and recovery in the event of a cyber breach, spanning investigation, remediation and recovery, backed by world-class threat intelligence and delivered by the most experienced IR team available.

Services Retainer | On-demand access to CrowdStrike expertise, from rapid response to long term resilience.

STRATEGIC ADVISORY SERVICES

Develop and mature the security program to improve defenses

Tabletop Exercises | Simulated incident response scenarios that expose process gaps and improve coordination across the full team, from hands-on-keyboard analysts to executive stakeholders.

Maturity Assessment | A comprehensive evaluation of an organization's security posture, identifying gaps, benchmarking capabilities, and providing a prioritized roadmap to strengthen defenses against evolving threats.

Regulation Readiness and CXO Advisory | Understand and prepare for cyber-related regulation mandates, including the evolving risk and governance responsibilities of the Board of Executives.

Insider Risk Program Review | Strengthen your insider risk strategy by assessing and optimizing your current detection, prevention, and response capabilities.

RED TEAM SERVICES

Test and validate defenses through emulated attacks that expose weaknesses

Penetration Testing | Attack emulations that test the detection and response capabilities of your people, processes and technology to identify vulnerabilities.

Red Team/Blue Team Exercise | Increase response readiness under our guidance, as a Red Team attacks systems in a simulated exercise and a Blue Team guides the defense.

Adversary Emulation Exercise | Gauge readiness to defend against a sophisticated adversary infiltration that employs advanced tradecraft.

AI Red Team Services | Expose vulnerabilities in the GenAI stack that could be exploited by testing LLM integrations for sensitive data exposure and adversarial manipulation.

TECHNICAL ASSESSMENT SERVICES

Audit and address security gaps across endpoints, cloud and SaaS applications to tangibly reduce risk

Technical Risk Assessment | Highlight security vulnerabilities, weaknesses and gaps in the IT environment across endpoint devices, applications and user identities.

Identity Security Assessment | Audit identity security practices and defense posture for weaknesses, including Active Directory domain configuration, account configuration, privilege delegation and potential attack paths.

Cloud Security Assessment | Identify misconfigurations and vulnerabilities in the cloud estate that could be exploited by adversaries.

Compromise Assessment | Expose and address undetected threat activity through a one-time threat hunt, available for endpoint, cloud and SaaS applications.

TRAINING AND SECURITY UPSKILLING

Build security acumen and close the skills gap through CrowdStrike University, including on-demand training, personalized learning paths, and five certifications for deep Falcon module expertise.

OUTCOME DELIVERED

CrowdStrike Professional Services stops the breach through elite IR and prepares organizations to avoid a breach through our expertise and a wide array of proactive security services.

- 5x reduction in recovery time from a breach. Source
- 10x reduction in recovery costs when breached. Source
- A clear path to security program maturity - avoid a breach scenario in the future through prepared people, polished processes, a capable strategy, and increased resilience.

Product Page: https://www.crowdstrike.com/en-us/services/

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.