CROWDSTRIKE

FALCON CLOUD SECURITY

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

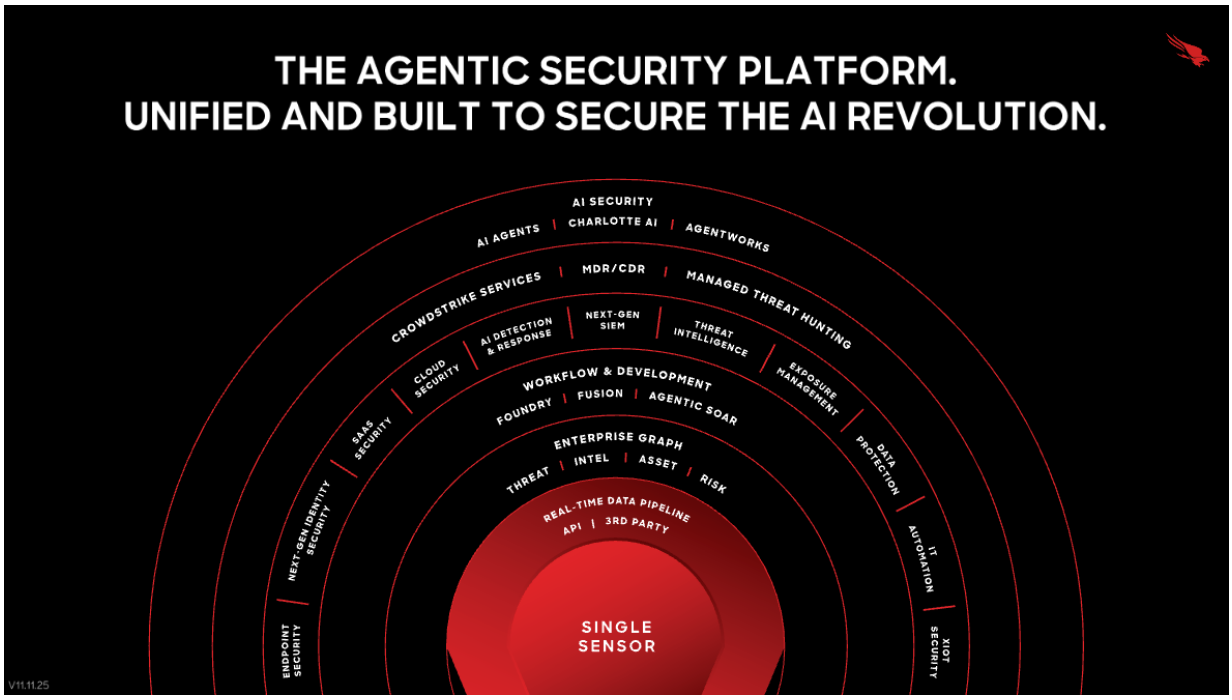
PLATFORM OVERVIEW

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 CLOUD SECURITY

CUSTOMER PROBLEM:

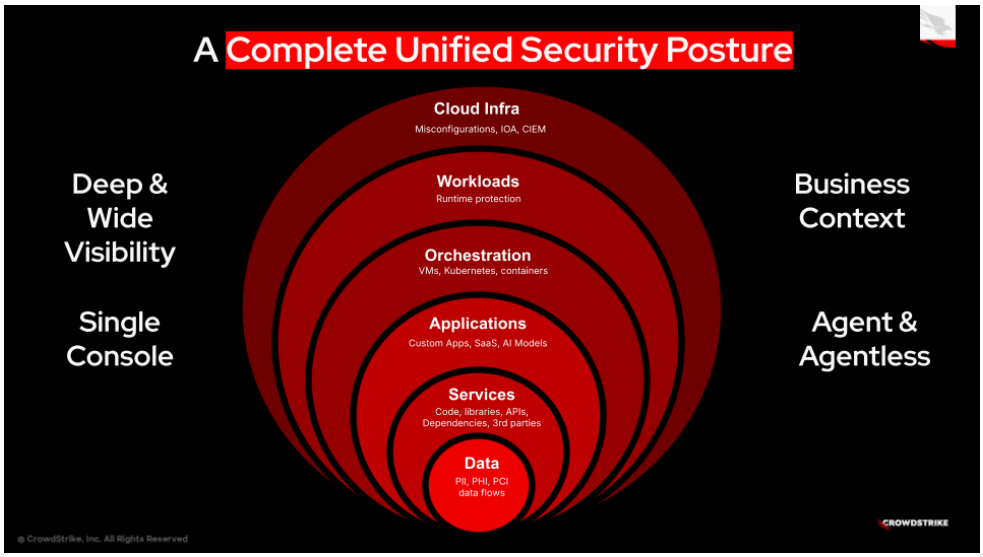
To secure the cloud, most organizations rely on a jigsaw of cloud security and vulnerability tools across on-premises and public clouds, covering individual layers like infrastructure, applications, APIs, data, AI, and SaaS. However, these tools create silos, lack integration, and generate overwhelming alert volumes, leaving teams with fragmented visibility and little context to prioritize risks. This leads to inefficiency, inter-team friction, lack of credibility, slow remediation, and reduced breach prevention.

Adversaries exploit this complexity, making it difficult for security to assess their security posture, detect cross-domain attacks (endpoint, identity, cloud), and stop breaches in dynamic hybrid environments. Groups like Scattered Spider and Labyrinth Chollima often initiate attacks via endpoints and stolen identities, escalating to hybrid cloud compromises to exfiltrate business-critical services and data.

WHAT'S NEEDED:

Organizations need cloud security solutions that bridge that gap between existing siloed platforms, provide enriched threat intelligence to detect key Indicators of Attack (IOAs), Indicators of Compromise (IOCs) and Indicators of Misconfigurations (IOMs) in order to stop sophisticated attacks. The keys to properly securing a hybrid cloud environment start with two critical components:

- **A Unified Cloud Native Protection Platform**: By bringing together posture management, with DevOps workflow integrations and pre-runtime security, teams can secure applications and data at scale across the entire cloud ecosystem. In this scenario customers can truly secure themselves across their entire cloud footprint. In addition, AI powered analysis can help teams prioritize what misconfigurations to fix first to reduce the attack surface in a targeted efficient manner.
- **Cloud Runtime Detection and Response**: Finally, once teams have visibility across their cloud and can fix vulnerabilities, they need real-time breach protection. That is why tools like Cloud Detection and Response (CDR) become critical. It's not enough just to know you have an intrusion, but can you stop it in time? That is why CDR has become so critical for true cloud protection.



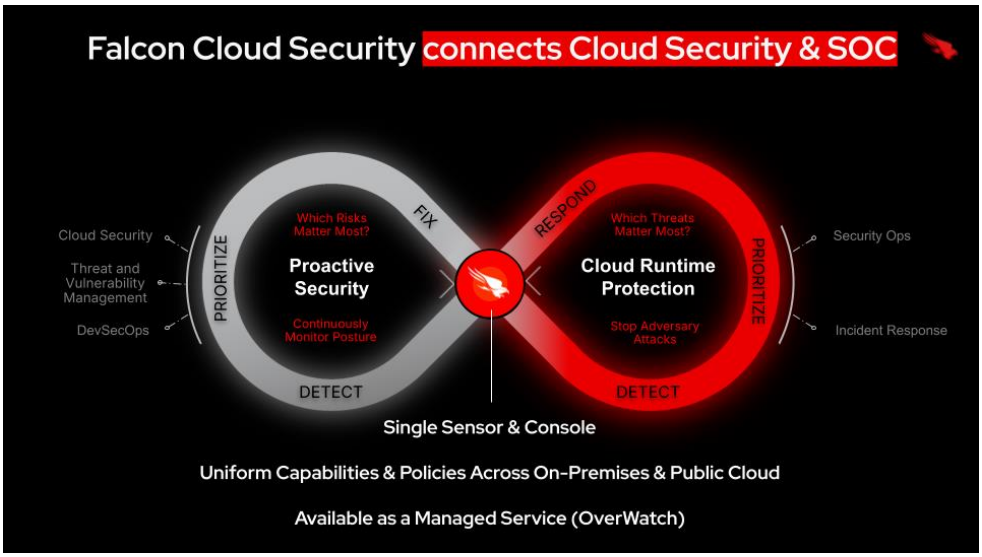
UNIQUE APPROACH:

CrowdStrike Falcon Cloud Security simplifies this complexity with a unified, best-in-class solution, a single sensor, and uniform policies that seamlessly provide proactive security and cloud runtime protection across on-premises and public clouds:

- **Proactive Security:** Unified cloud security posture (USPM) and business context across cloud layers, leveraging industry leading threat intelligence, end-to-end attack paths, and ExPRT.AI to reduce alert noise by 95%. Cloud and TVM teams can swiftly prioritize their work, neutralize critical risks, and leave adversaries no room to strike.
- **Cloud Runtime Protection:** Delivers best-in-class cloud runtime workload protection (CWP) and cloud detect and response (CDR), allowing SOC teams to detect and respond to active threats across hybrid clouds so adversaries are stopped in their tracks.

CrowdStrike offers both proactive and protective security as a managed service (MDR) through **Falcon Overwatch and Falcon Complete** powered by our cross-domain threat hunting team and counter adversary operations who protect the cloud control plane, host OS, and data plane.

CrowdStrike Falcon Security combines Proactive Security and Cloud Runtime Protection to bring cloud and security operations teams together, creating a powerful flywheel effect. This collaboration enhances visibility, streamlines risk prioritization, and enables effective remediation. By adopting this unified approach, organizations continuously improve their security posture, boost operator productivity, cut costs, and outpace modern adversaries to prevent breaches.



OUTCOME DELIVERED:

Customers using **CrowdStrike Falcon Security** typically achieve the following business outcomes:

- 72% faster ability to monitor the entire cloud estate
- 89% faster cloud detection and response
- 83% reduction in cloud security licenses due to elimination of redundant tools
- $380k saved annually on average using FCS
- 65 hours saved on average per month (1 FTE for one week per month)
- 71% improvement in policy consistency across the cloud estate

Product Page: https://www.crowdstrike.com/platform/cloud-security/

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.