CROWDSTRIKE

FALCON ENDPOINT 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

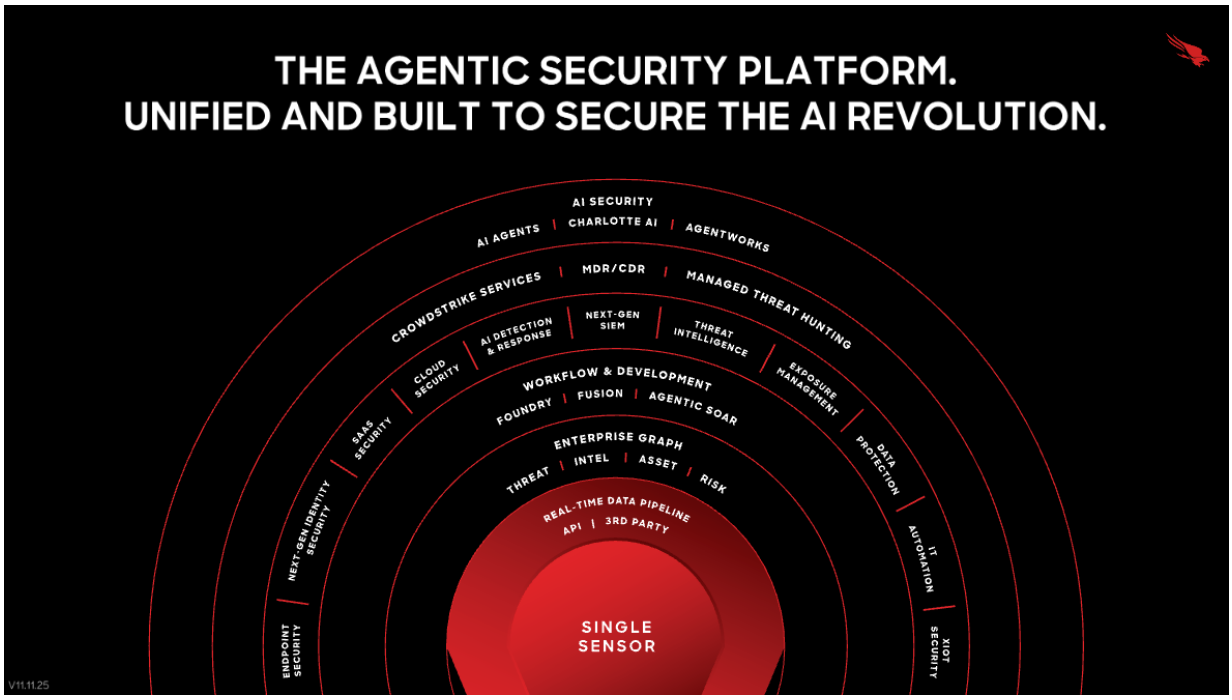
PLATFORM OVERVIEW

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.

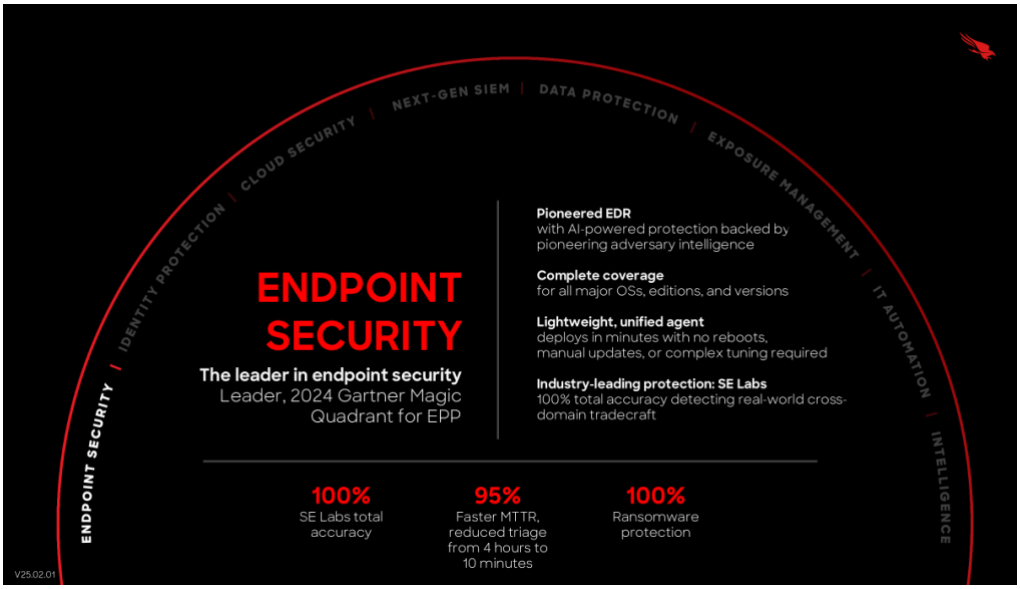
Infused with AI expertise
At CrowdStrike, AI is more than a feature — it's in our DNA. With models trained on trillions of data points every day, we predict and stop threats in their tracks.

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 INSIGHT XDR: ENDPOINT DETECTION AND RESPONSE



CrowdStrike Falcon® Insight XDR delivers continuous and comprehensive visibility that spans detection, response and forensics for endpoints and beyond to stop potential breaches.

CUSTOMER PROBLEM:

Modern adversaries are moving faster than ever. The fastest breakout times measured by CrowdStrike indicate that defenders have mere minutes to see and stop advanced threats before significant damage is done to an organization. It is not enough for organizations to try and outright block every threat; attackers are evolving to become more evasive, less reliant on malware and increasingly fond of trusted tools that already exist in an organization's environment. When an attacker uses these methods to blend in with legitimate activity, security teams often lack actionable data and insights to quickly identify malicious activity and respond accordingly. Security teams need to be able to easily correlate this data with security context from other key domains to stop advanced attacks and minimize business downtime.

WHAT'S NEEDED:

Security teams need detection and response technology that can provide the highest level of protection while requiring the least amount of effort and investment, adding value to security operations without draining resources.

Enterprise-wide visibility: Real-time visibility across all endpoints uncovers adversary activities, even as they attempt to breach the environment, and stops them immediately.

Comprehensive native endpoint data: Effective, unified EDR/extended detection and response (XDR) requires comprehensive telemetry collected from as many endpoints as possible and enriched with cross-domain context so it can be mined for signs of attack with a variety of analytic techniques.

AI-powered detection: Relying solely on signature-based methods or IOCs leads to the "silent failure" that allows data breaches to occur. Effective endpoint detection and response requires AI-powered

behavioral approaches that search for IOAs so that you are alerted of suspicious activities before a compromise can occur.

Actionable insights and intelligence: An EDR solution that integrates threat intelligence can provide context, including details on the attributed adversary that is attacking you or other information about the attack.

Fast response: Unified EDR/XDR that enables a fast and accurate response to incidents can stop an attack before it becomes a breach and allow your organization to get back to business quickly.

UNIQUE APPROACH:

With these sophisticated attacks moving quickly and becoming more evasive, stopping modern breaches requires the right data, rich context and the ability to move faster than the adversary. Falcon Insight XDR provides comprehensive, enterprise-grade endpoint visibility with AI-powered detections and rapid response capabilities. Falcon Insight XDR continuously monitors endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to detect advanced threats as they happen.

Falcon Insight XDR accelerates security operations, allowing users to reduce the time they spend handling alerts and quickly investigate and respond to attacks. The all-new Incident Workbench delivers AI-powered workflows, enabling seamless investigations with innovative collaboration so security teams can hunt, detect and respond to attacks as a cohesive unit.

Falcon Insight XDR also provides a unified EDR/XDR experience that spans multiple domains of key native security telemetry. CrowdStrike's data is augmented with market-leading threat intelligence to reveal even the stealthiest of attacks, and analysts of all skill levels benefit from scalable automation tools across the platform, including native response actions for other supported Falcon platform modules.

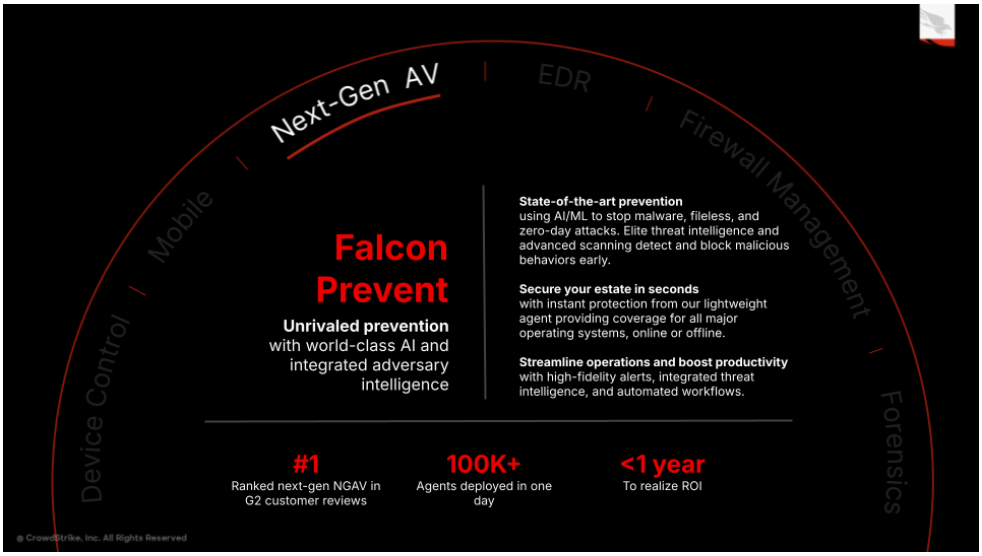
OUTCOME DELIVERED:

Falcon Insight XDR transforms security teams struggling with missed attacks and slow response to a modern SOC with unbeatable protection and immediate ROI.

- **100%** detection accuracy with zero false positives in the Q3 2024 SE Labs Enterprise Advanced Security test
- **95%** reduction in MTTR, speeding triage from 4 hours to 10 minutes (customer case study)
- **100%** ransomware protection in the 2024 SE Labs Enterprise Advanced Security (EDR) Ransomware test

Product Page: https://www.crowdstrike.com/platform/endpoint-security/falcon-insight-xdr/

FALCON PREVENT: NEXT-GENERATION ANTIVIRUS



CUSTOMER PROBLEM:

The antivirus software market is evolving from traditional signature-based detection methods to advanced NGAV solutions. Traditional antivirus software focuses on identifying known malware through signature comparisons and heuristic analysis. However, it often struggles with newer, sophisticated threats. The lack of comprehensive, proactive protection leaves critical endpoints vulnerable, increasing the risk of data breaches. NGAV solutions enhance cybersecurity by employing behavioral analysis, machine learning and cloud-based threat intelligence, providing proactive and comprehensive protection against advanced threats like zero-day exploits, fileless attacks and ransomware.

WHAT'S NEEDED:

- Customers need comprehensive protection against advanced modern threats that evolve faster than traditional antivirus solutions can adapt. Legacy antivirus products, which primarily rely on signature-based detection, fall short when it comes to defending against sophisticated threats like zero-day exploits, ransomware and advanced persistent threats (APTs). With the rapid evolution of these attack vectors, customers require security solutions that offer proactive, real-time threat detection and prevention to safeguard their systems and data from potential vulnerabilities.
- Customers need efficient security solutions that don't compromise system performance or productivity. Traditional antivirus solutions often consume substantial system resources due to frequent signature updates and extensive scanning processes, resulting in performance degradation. This can cause system lag and reduced efficiency, particularly in resource-constrained environments, impacting overall productivity. Customers require a lightweight solution that provides robust protection without sacrificing the speed and efficiency of their systems.
- Customers need security solutions with integrated threat intelligence and enhanced visibility into the evolving threat landscape. Legacy antivirus solutions often lack these capabilities, leaving organizations unaware of the full scope of potential attacks and hindering their ability to proactively respond to emerging threats. Without real-time threat intelligence, security teams are left guessing about the nature of attacks, who is targeting them and why, forcing a reactive approach rather than proactive prevention. To stay ahead of attackers, customers require solutions that offer actionable insights and real-time threat analysis to mitigate risks effectively.

UNIQUE APPROACH:

CrowdStrike® Falcon Prevent® offers an AI-powered NGAV solution that integrates advanced threat intelligence and machine learning to provide comprehensive, proactive protection. With its lightweight agent architecture, Falcon Prevent effectively prevents known and unknown cyberattacks without the need for constant signature updates or complex integrations, providing robust security for organizational digital assets.

- **Advanced Threat Detection and Prevention**
  - Falcon Prevent leverages AI-driven technology and integrated threat intelligence to detect and prevent a wide range of advanced threats, including zero-day exploits, ransomware and sophisticated malware. By using machine learning to analyze behavior patterns and identify anomalies, Falcon Prevent provides proactive and comprehensive protection that goes beyond traditional signature-based methods.
- **Lightweight Agent Architecture**
  - Falcon Prevent is designed with a single lightweight agent that operates efficiently without consuming excessive system resources. This architecture minimizes performance impact on endpoints, ensuring that users can maintain productivity without experiencing system slowdowns or lag. The lightweight design also makes it suitable for resource-constrained environments.
- **Modern Threat Detail**
  - Falcon Prevent integrates real-time threat intelligence directly into its NGAV platform, providing comprehensive visibility into the threat landscape. This empowers security teams with instant insights into potential attacks and adversaries, enabling proactive defense measures. With enhanced visibility and intelligence, organizations can swiftly prioritize responses, mitigate risks and stay ahead of emerging threats.

OUTCOME DELIVERED:

- 100% ransomware protection (Commercial Bank of California)
- **StepStone** trusts CrowdStrike to protect jobseeker data:
  - "In simple terms, other solutions and antivirus products work by identifying the 'mugshot' of a known threat rather than tracking suspicious activity. As CrowdStrike is heuristic, it looks at behavior as well as at the mugshot." — Serge Groven, Senior Corporate IT Manager, StepStone
  - 3,600 endpoints deployed in six weeks
  - Overhead dropped to under 1% of endpoint processing power

- **Autoglass/Maxpar**: Leading Brazilian automotive business saves time and increases efficiency by securing operations with CrowdStrike:
  - "What caught our attention about CrowdStrike was agility. CrowdStrike was quick to install and easy to use, and feedback from staff was super positive. Most importantly, the product showed it could solve one of our main challenges: visibility of the environment." — Fabiano Moura, IT Executive Manager, Autoglass/Maxpar

- **Guararapes Group**: Brazilian fashion and retail business protects 30 million customers' financial data with CrowdStrike solutions:
    - "My greatest difficulty before CrowdStrike was having visibility to attacks in real time. And since CrowdStrike does not need constant updating, it is able to spot new malware and viruses automatically. Before, these threats could sit there quietly on a machine waiting to attack. Greater visibility means we can respond faster to these malicious attempts and incidents." — Rodrigo Godoi, CISO, Guararapes Group

Product Page: https://www.crowdstrike.com/platform/endpoint-security/falcon-prevent-ngav/

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.