CROWDSTRIKE

FALCON NEXT-GEN SIEM

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

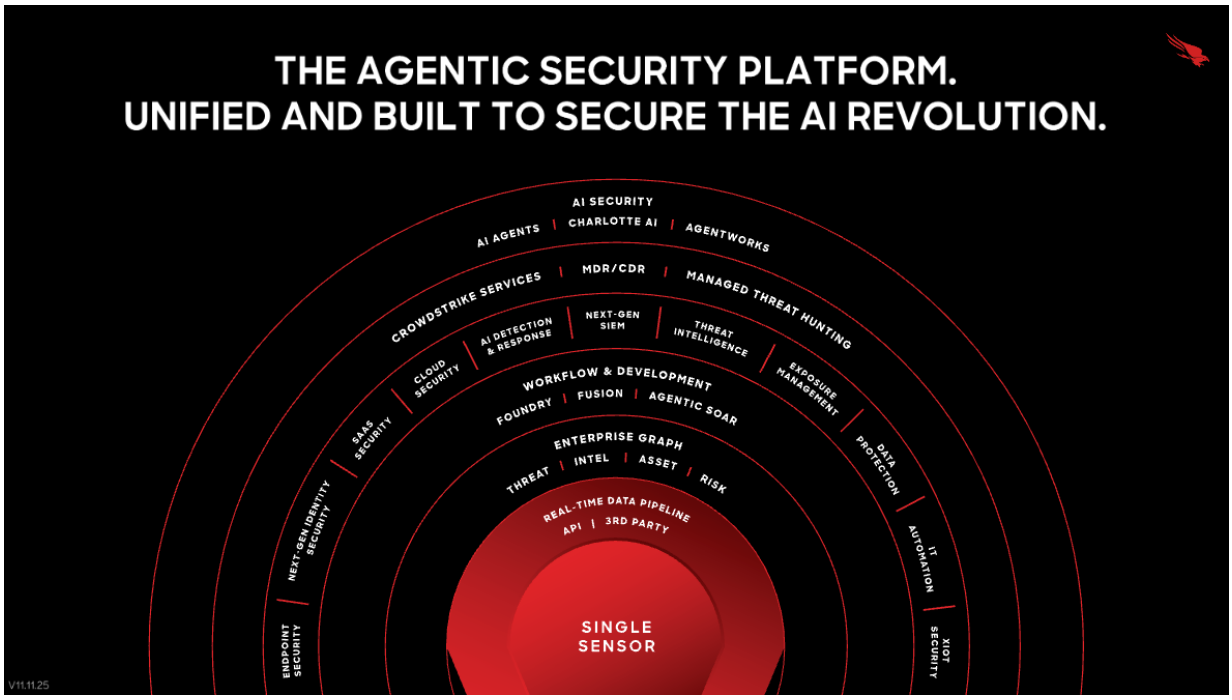
PLATFORM OVERVIEW

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 NEXT-GEN SIEM

CUSTOMER PROBLEM:

Stopping modern attacks requires SecOps teams to match the speed of the adversary. But as attack velocity and stealth increase, the legacy SIEM tools of the past have failed to adapt. Slow, complex and costly, they were designed for an age that's long since passed, when data volumes and adversary speed were a fraction of what they are today. Soaring SIEM costs compound these challenges by preventing teams from logging and retaining all of their data, resulting in blind spots and missed attacks.

To give security teams the speed they need to stop breaches, the modern SOC requires a platform that converges data, security and IT, with AI and workflow automation built natively within.

WHAT'S NEEDED:

Protectors need an edge that's orders of magnitude faster, easier to deploy and far more cost effective than current approaches. To stop modern adversaries, the SIEM needs to be rebuilt for the SOC from the ground up, centered around the security analyst experience, to deliver better, faster and more cost-effective outcomes that stop breaches. By unifying threat detection, investigation and response capabilities in one cloud-native, scalable platform, next-gen SIEM will:

- Accelerate time-to-value by onboarding data from any source with ease: Next-gen SIEM must start with unified, native data across endpoints, cloud workloads, identities and data protection, augmented with easy-to-connect third-party sources.
- Automate incident response with AI-led investigations: Investigations will move from manual, slow searches to AI-created incidents that automatically stitch together all related alerts and context, summarize them in plain language with generative AI, and make it easy to understand the full scope of an attack through an elegant yet powerful visual graph.
- Let you respond in real time: You'll be able to stop attacks in seconds instead of days by automating detection, investigation and response workflows with integrated orchestration capabilities.
- Unlock search at lightning speed: Searches must be measured in fractions of a second, not minutes or hours.

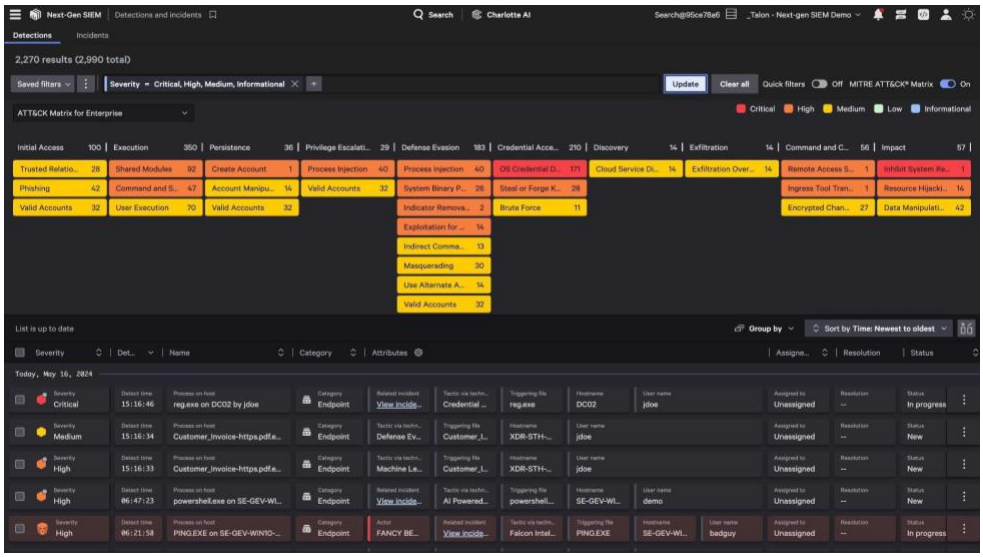
- Drive smarter decisions with native adversary context: All key information on the adversary and their tradecraft must be instantly available within the platform.
- Eliminate the skills gaps and automate manual actions with generative AI: Security analysts of any skill level must be able to use plain-language prompts and generative AI workflows for any task.
- Minimize costs: Don't compromise on security by limiting data retention due to high cost by collecting and storing all data, at petabyte scale, at a much higher ROI.

UNIQUE APPROACH:

With CrowdStrike Falcon® Next-Gen SIEM, CrowdStrike is unifying the SOC to stop breaches faster than ever before. Falcon Next-Gen SIEM extends the world's leading detection and response, threat intelligence and expert services to all data for complete visibility and protection. It enables full visibility across all streaming logs and event data and helps customers cut incident response times by streamlining investigations with built-in automation and generative AI. As a unified, AI-native platform, Falcon Next-Gen SIEM will boost your threat detection, investigation and response with unrivaled speed and efficiency.

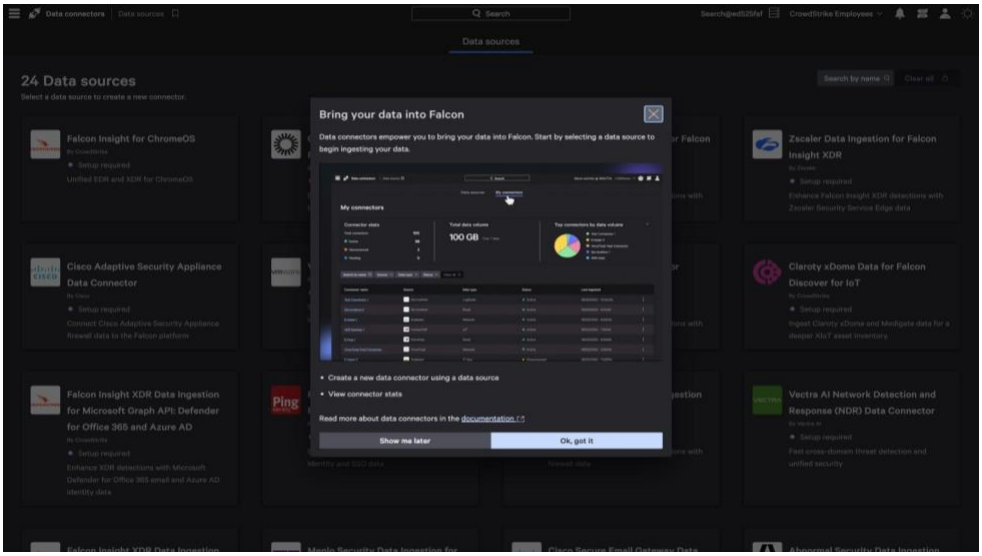
Falcon Next-Gen SIEM delivers:

- **A powerful, AI-native SOC platform:** CrowdStrike brings together the next generation of SIEM technology with industry-leading EDR, identity protection, cloud security and threat intelligence on one platform with one console to cut complexity and costs. With Falcon Next-Gen SIEM, you can ingest, aggregate and analyze massive volumes of streaming log data at scale due to its cloud-native architecture, which delivers superior performance and scalability to grow with your data volumes. Falcon Next-Gen SIEM supports a variety of use cases, including detection, forensics, incident response and remediation, impact assessment, threat hunting and compliance.

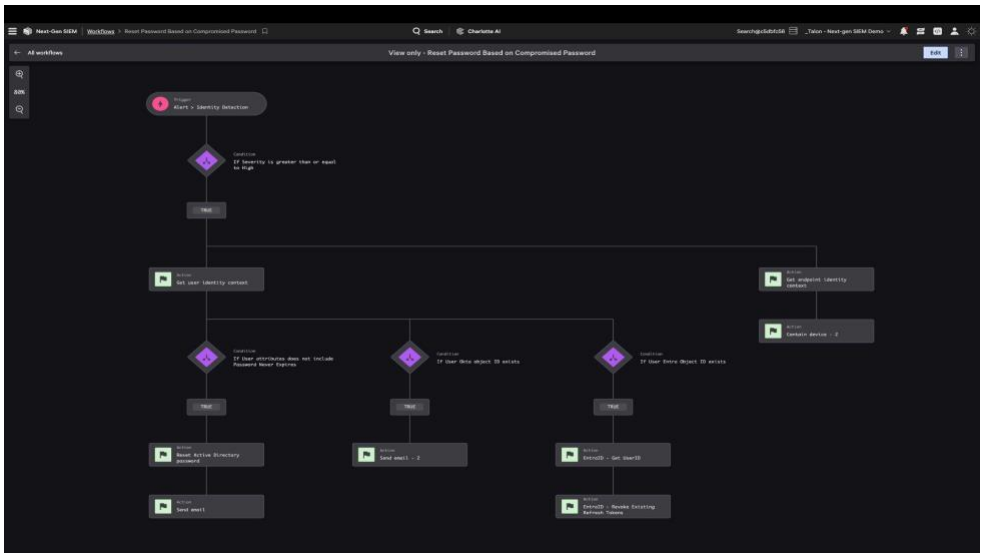


- **Immediate value with simplified data onboarding, analytics and high-fidelity detections:** Falcon Next-Gen SIEM easily collects data from any source with a growing set of ingestion methods and connectors. With its sub-second latency and index-free search, Falcon Next-Gen SIEM gives your team instant visibility into all of your data, including the endpoint, identity and cloud workload data

that already exists in the Falcon platform. Data inside Falcon Next-Gen SIEM is easy to analyze, with a broad spectrum of data operations and different ways — such as search, aggregation and visualizations — to delve deeper into the data. The search capabilities of Falcon Next-Gen SIEM range from simple to advance to provide value to end users of all skill levels. Search queries can easily be turned into dashboards that offer a variety of widgets, and these dashboards can be exported via PDF so you can share them with anyone on the team. Falcon Next-Gen SIEM also empowers you to find the most sophisticated adversaries across all data sources with cross-domain detections powered by the same advanced AI and behavioral analysis as CrowdStrike's industry leading endpoint detection, investigation and response.



- **Fully integrated security orchestration, automation and response to free up your team to focus on high-priority operations**: Falcon Next-Gen SIEM speeds up investigation and response with tightly integrated threat intelligence, workflow automation and generative AI. Falcon Next-Gen SIEM leverages Falcon Fusion SOAR, CrowdStrike's native workflow automation solution, to automate and orchestrate investigation and remediation actions across the Falcon platform and third-party tools — all from one unified console. It is also tightly integrated with the Falcon agent to drive any endpoint action — through Falcon RTR — to contain fast-moving attacks.



- **A modern security analyst experience to up-level security analysts:** Falcon Next-Gen SIEM doesn't just aggregate, alert on and visualize data in real time and at scale — with its incident management and AI capabilities, it elevates security analysts to become more productive and efficient. Falcon Next-Gen SIEM enables lightning-fast investigations by providing complete context, and analysts can understand an adversary's entire attack path through a visual graph that allows for real-time collaboration. Additionally, analysts can leverage AI-native features — like Charlotte AI — to help stitch together all of the related alerts, context and industry-leading threat intelligence in a plain-language summary. Charlotte AI, the ultimate force multiplier, also allows analysts to ask questions to streamline investigations with the power of high-fidelity data and generative AI.

OUTCOME DELIVERED:

CrowdStrike Falcon Next-Gen SIEM delivers superior security outcomes; lower costs compared to siloed SOC tools and seamlessly extends the capabilities of the world-leading CrowdStrike Falcon platform.

- **Modernize your SOC:** Achieve complete SOC transformation with a modern analyst experience and unrivaled security outcomes, at a fraction of the cost of traditional SIEMs. CrowdStrike unifies Falcon and third-party data, threat intelligence, AI and workflow automation to deliver unprecedented speed and efficiency to security teams to stop breaches.
- **Search up to 150x faster to stop attacks before the damage is done:** Avoid costly breaches by slashing incident response times with real-time alerting, blazing-fast search and automated workflows to eliminate threats before the damage is done.
- **Get faster time-to-value and scale out your logging capacity in hours rather than weeks:** Extend the retention of your key security data with a few clicks and experience rapid ROI. A growing set of data integrations lets you easily onboard data from any source. Plus, since it's an elastic, cloud-native platform, Falcon Next-Gen SIEM lets you easily collect more data without the hassle of deploying new servers, storage, monitoring and backup devices.
- **Achieve up to 80% cost savings by replacing your legacy SIEM:** Unify threat detection, investigation and response in one AI-powered, cloud-native platform to streamline operations and reduce complexity and costs. Boost analyst efficiency by automating repetitive tasks and minimizing alert fatigue and swivel-chair syndrome.

Product Page: https://www.crowdstrike.com/platform/next-gen-siem/

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.