CROWDSTRIKE

FALCON XIoT 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

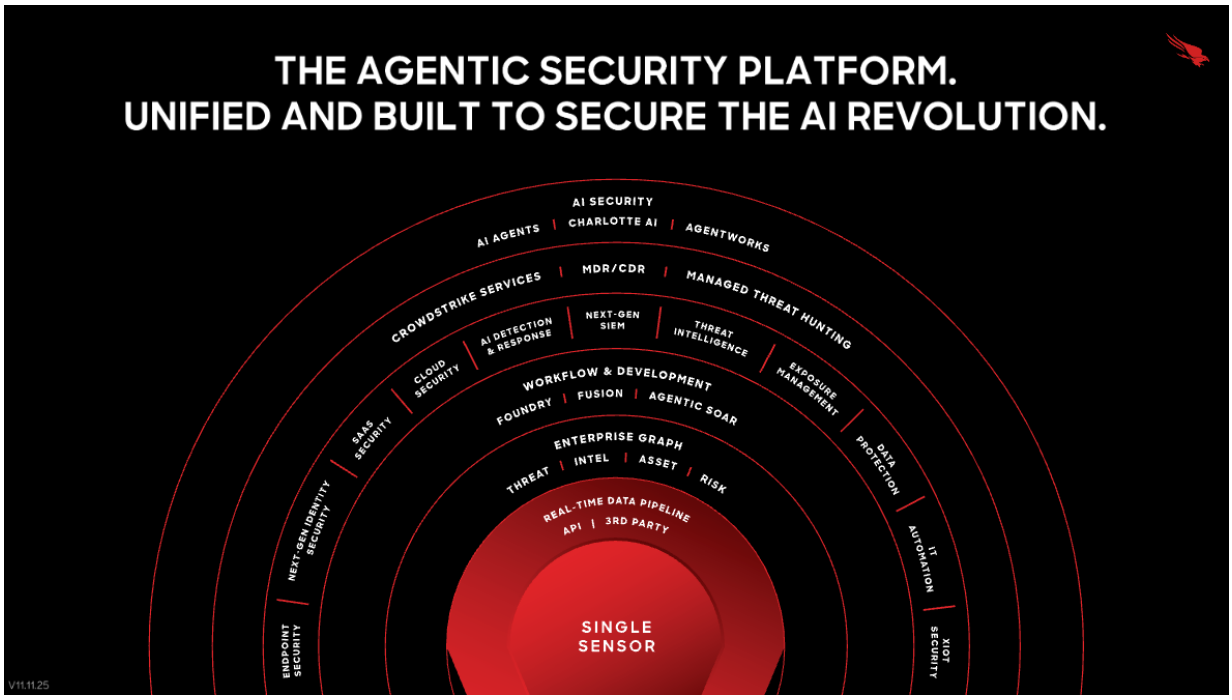
PLATFORM OVERVIEW

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 DISCOVER FOR IOT

CUSTOMER PROBLEM:

For any environment, securing assets must start with comprehensive visibility — you can't protect what you can't see. Customers struggle to gain complete visibility into their IoT/OT assets due to technology and resource constraints. As sophisticated, low-cost attacks against IoT/OT assets rise, the need to see these assets and risks is paramount.

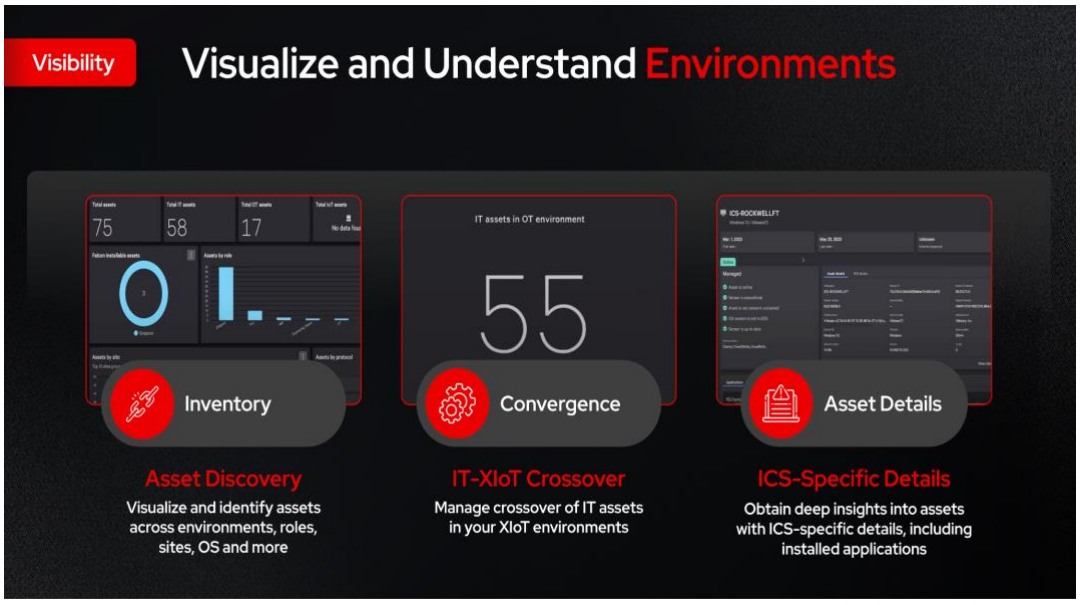
WHAT'S NEEDED:

Organizations need to get complete IoT/OT asset and vulnerability visibility without the complexity and cost associated with new vendors and hardware deployments.

UNIQUE APPROACH:

Building on industry-leading visibility and protection in IT environments, Crowdstrike helps organizations secure their industrial control system (ICS) environments and embrace operational technology (OT) digital transformation with comprehensive visibility into extended internet of things (XIoT) assets, including IoT, OT, internet of medical things (IoMT), industrial internet of things (IoT) and Industry 4.0 assets.

CrowdStrike Falcon® Discover for IoT eliminates XIoT blind spots to proactively stop breaches, helps organizations break ICS environment silos and delivers superior ROI from a trusted and easy-to-manage platform.



KEY BENEFITS OF FALCON DISCOVER FOR IOT:

Complete, unified asset visibility in ICS environments:

- Identify all managed and unmanaged IoT, OT and IT assets in ICS environments
- Unify asset visibility across endpoints and networks into a single platform, utilizing native capabilities and/or robust integrations with partners like Claroty and Dragos
- Immediately find specific assets in the environment by filtering on device, criticality, Purdue level, site, protocol and operating system

Complete visibility in 10 minutes or less:

- Quickly discover IoT, OT and IT assets in ICS environments without any hardware or time-consumingly and complex network configuration changes
- Schedule asset collections on the interval of your choice for easy, hands-off visibility
- Get detailed asset information, including device type, manufacturer, site name, device class and more
- Uncover unprotected assets that need a Falcon agent to keep your organization protected from advanced threats

Rapid OT threat investigation and response:

- Better understand the attack surface with detailed, real-time asset relationship mapping across converging OT and IT environments
- Uncover hidden threats by quickly identifying how assets interact with each other throughout the environment
- Speed investigation and response by drilling into essential asset details like related entities, internet exposure and more

OUTCOME DELIVERED: Falcon Discover for IoT delivers:

- Complete IoT/OT visibility in **10 minutes or less**.
- Vulnerability prioritization and remediation guidance to help streamline and close vulnerabilities faster.

Product Page: https://www.crowdstrike.com/en-us/resources/data-sheets/falcon-discover-for-iot/

FALCON INSIGHT FOR IOT

CUSTOMER PROBLEM:

Organizations have traditionally relied on "air-gapped" IoT/OT environments. As IoT/OT has proliferated, while requiring interconnectedness with IT environments, the notion of the air gap has largely gone away. To combat the risks associated with assets that are now exploitable, organizations need to understand the risk their assets pose, while preventing and detecting targeted IoT/OT attacks.

WHAT'S NEEDED:

Organizations need comprehensive NGAV, EDR, and XDR capabilities for their IoT/OT assets.

UNIQUE APPROACH:

CrowdStrike Falcon® Insight for IoT is built to stop breaches for XIoT assets, delivering tailored threat prevention, detection and response that won't disrupt operations. Rigorous testing of CrowdStrike's lightweight Falcon agent by leading ICS vendors underscores its benefits: fast and simple deployment, comprehensive interoperability and safety for mission-critical XIoT assets. Falcon Insight for IoT extends world-class protection across the entire enterprise, removes blind spots by breaking down IT/OT silos and delivers best-in-class ROI.

KEY BENEFITS OF FALCON INSIGHT FOR IOT:

Stop XIoT threats at the source:

- Stop threats at the source with tailored threat prevention policies for XIoT assets
- Reduce performance impact to ensure the effectiveness, interoperability and safety of XIoT assets
- Easily manage sensor updates so you have time to test before deploying

Reduce risk with powerful XIoT detections:

- Reduce risk by detecting threats to XIoT assets, with deep context powered by AI, ML and actionable threat intelligence
- Provide Business continuity by identifying threats like ransomware and malicious project file modifications
- Build a cohesive picture of threat activity with telemetry ingested and analyzed across your enterprise
- Enable rapid, proven response for hard-to-patch assets:
- Limit the attack blast radius by blocking traffic and containing compromised hosts and processes without disrupting operations
- Safeguard operations from ransomware by limiting/revoking access to project files
- Streamline operations with response actions through third-party tools — like Claroty, a CrowdStrike Marketplace partner that helps secure cyber-physical systems — and automate repetitive tasks with Falcon Fusion SOAR

OUTCOME DELIVERED: Falcon Insight for IoT delivers:

- Complete protection of IoT/OT assets by fusing rich asset context with industry-leading threat detection and prevention.
- Compliance with IoT/OT asset standards as set by ICS vendors, ensuring safety, availability and interoperability with other mission-critical systems.

Product Page: https://www.crowdstrike.com/products/iot-security/falcon-insight-iot/

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.