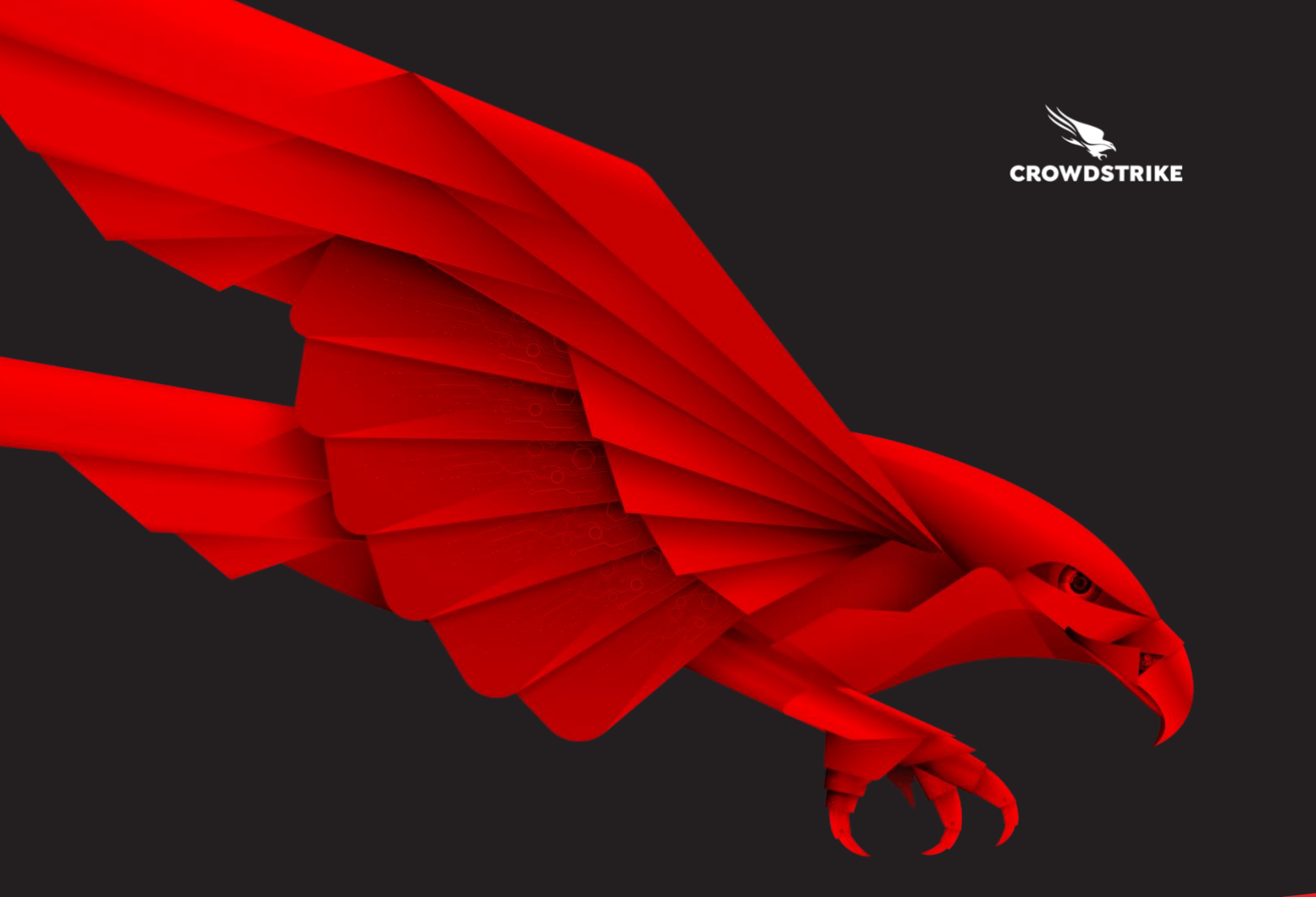


# FALCON EXPOSURE MANAGEMENT

IN RESPONSE TO

## G-Cloud 14 Framework (Lots 1-3)

Service Description

150 MATHILDA PL SUITE 300, SUNNYVALE, CALIFORNIA 94086
TEL: (888)512-8906 | FAX:(949) 417-1289
HTTPS://WWW.CROWDSTRIKE.COM/PRODUCTS/OBSERVABILITY/FALCON-LOGSCALE/

# DOCUMENT CONTROL

| | |
|---|---|
| Date | **04.2024** |

## CROWDSTRIKE CONTACT

| | |
|---|---|
| Account Manager | Peter Carthew<br>Regional Sales Director<br>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.

# TABLE OF CONTENTS

# 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.

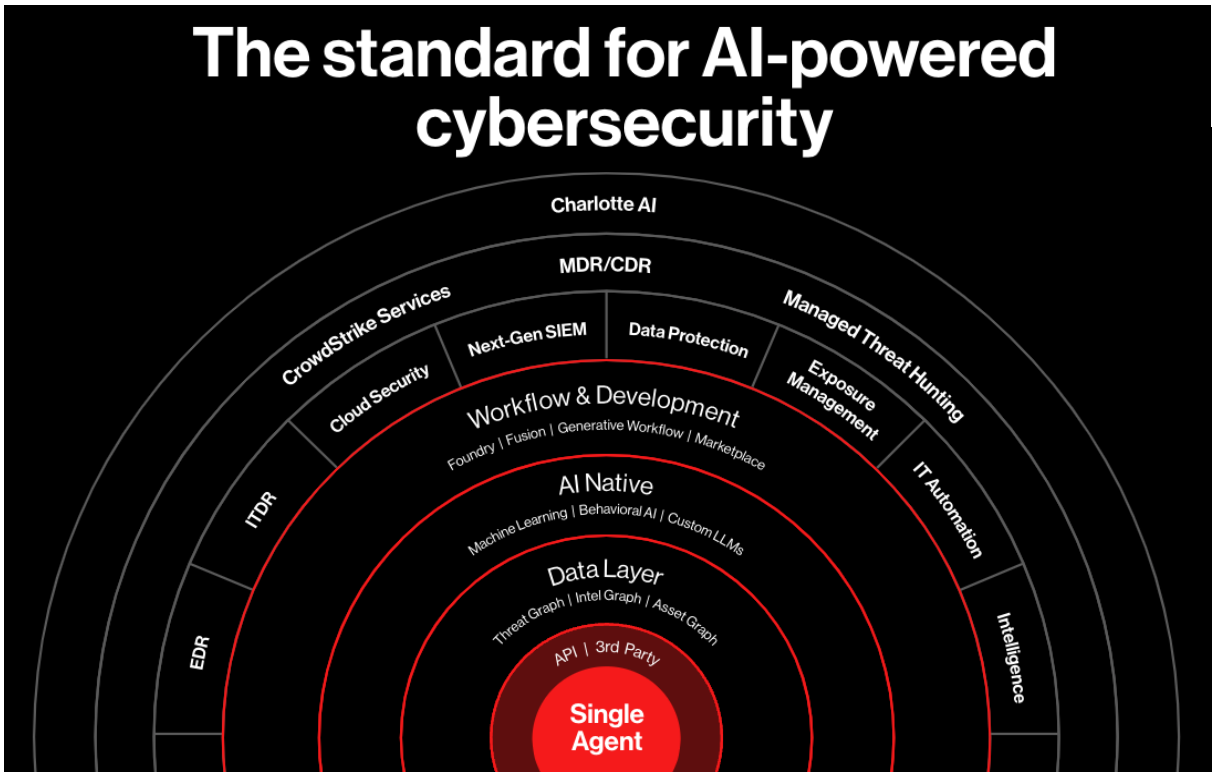
Infused with AI expertise

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.

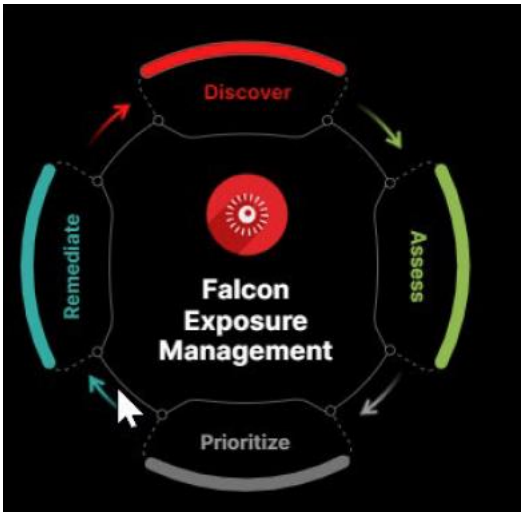
Effortless workflows and automation

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 EXPOSURE MANAGEMENT




**The world's leading AI-powered platform for exposure management.**

Proactive vulnerability and risk management can be a formidable undertaking in the best of times, in no small part due to the maintenance-intensive nature of many traditional vulnerability management (VM) tools. These tools often take weeks or even months to complete a single scan, while also demanding constant upkeep and care. Adding to that struggle, the proliferation in type and modality of IT assets has created an explosion of new and ever-shifting attack surfaces. For many security teams, merely knowing what they are responsible for protecting can be a serious challenge, not to mention developing a holistic understanding of these assets, the associated exposures and adversary context. Point solutions attempting to address this can themselves represent another source of fragmentation. As many practitioners know, understanding the asset landscape is half of the battle in effective security. Furthermore, while the ultimate goal for CISOs and boards of directors is to prevent breaches, most VM tools operate in a silo, lacking meaningful integrations with real-time security tools and the associated benefit of insight and mitigation. With the increasing prominence of zero days and high-profile exploits, this tooling gap often hampers cross-security collaboration, impeding timely and synchronized actions and leaving more opportunity to attackers.

**Key Challenges**

- Legacy VM tools come with a maintenance burden and require slow, disruptive scans
- Security teams struggle to discover and understand overall attack surfaces and
- adversary context
- Fragmented solutions and lack of visibility impede holistic prioritization and undermine
- security posture
- Siloed risk management tools stop at understanding risk and are unable to stop breaches

CrowdStrike Falcon® Exposure Management is a powerful ground-breaking product that harnesses the cutting-edge capabilities of the CrowdStrike Falcon® platform. This innovative solution utilizes the unified, lightweight Falcon agent, which enables real-time, maintenance-free vulnerability assessment. Moreover, it integrates the robust, predictive ExPRT.AI prioritization model, trained on world-class threat intelligence and real-life threat detection incidents. These features empower security teams to allocate their limited resources strategically, focusing 95% of resources on the 5% of risk exposures1 that are most likely to be exploited by threat actors. In addition, Falcon Exposure Management offers unparalleled real-time asset discovery and understanding, extensive exposure assessment and consolidated visibility across the entire attack surface. This comprehensive suite of capabilities assists organizations in effectively staying on top of their internal and external asset exposures, reducing the external attack surface by 75%,2 mitigating risks and fostering effective collaboration within the security team. By combining Falcon Exposure Management with CrowdStrike's cutting-edge, real-time security solutions, organizations can safeguard their systems against potential attackers and maintain a strong proactive security posture.

## KEY CAPABILITIES

Falcon Exposure Management helps security teams fully operationalize vulnerability management programs through the entire lifecycle, from the foundational aspect of asset discovery, to assessment and prioritization of vulnerabilities and exposures, all the way to effective remediation.

## DISCOVER

Thoroughly discover all of your assets and blind spots with a variety of advanced methods including active discovery and external attack surface management (EASM). Gain additional context through intelligence such as asset roles, criticality and possible internet exposures.

**Active, Passive and API-based Asset Discovery**
Effortlessly discover all of the assets in your environment whether they reside on-premises, in the cloud, IT, OT/IoT, endpoint, workloads or applications. Rather than deploying onerous network scanning appliances, the unified CrowdStrike Falcon agent can be designated as a scanner to conduct active asset discovery scans of the network. Passive discovery, on the other hand, utilizes CrowdStrike Falcon® Insight XDR telemetry and local host information such as ARP tables and DNS cache, allowing for automatic understanding of your network segments. API-based discovery allows for asset data ingestion from third-party sources such as ServiceNow, Claroty, Active Directory and many others.

**External Attack Surface Management (EASM)**
Exposure to the public internet is often an organization's blind spot, and it's frequently the attacker's first stop. Get an outside-in view of the enterprise attack surface and discover internet-connected assets that were previously unknown. Using a proprietary internet mapping technology operating 24/7, the EASM engine can determine location information and see real-time changes. It also automatically provides business discovery, including mapping subsidiaries and other M&A activities.

**Application, Account and Identity Intelligence**
Track installed applications on each asset. See details of how applications are being utilized and whether unauthorized software is installed. Monitor which accounts are being used, how domain and local credentials are being accessed, when passwords are changed and other potentially suspicious activity.

**Asset Roles**
In an enterprise environment with tens of thousands of assets, it is not always easy to determine which machine does what, given disparate ownerships and scattered geography. Falcon Exposure Management can automatically determine an asset's role based on its behaviors and activity level, such as when a machine is a DHCP server, email server or a jump server, providing essential context for better understanding risk and exposure.

## ASSESS

Effortlessly assess for a wide variety of exposures. Build compliance using CIS benchmarks. Ingest third-party sources of vulnerability information so you can master your entire exposure surface in one place without needing a separate cyber asset attack surface management (CAASM) tool.

**Native Scanless Vulnerability Assessment**
Continuous vulnerability assessment using CrowdStrike's single, multi-functional, lightweight Falcon agent provides real-time visibility with no infrastructure overhead or maintenance. Get wide-ranging vulnerability coverage including software CVEs, misconfigurations and end-of-support-life detection on Windows, MacOS, Linux and related applications. Obtain rich vulnerability details, exploit information and attacker context through multitudes of first-party and third-party intelligence feeds.

**Secure Configuration Assessment (SCA) against CIS Benchmarks**
Weakly configured or misconfigured assets are just as susceptible to threats as those with software vulnerabilities. Assess your assets' configuration settings against user-customizable CIS Benchmarks (a comprehensive set of prescriptive best practice standards), whether for compliance objectives or up-levelled security.

**Third-party Vulnerability Data Ingestion**
Ingest vulnerability information from third-party scanning solutions and see them alongside CrowdStrike's native vulnerability data to create a single pane of glass for prioritizing and operationalizing all of your exposure information, without the need to pay for a separate integration tool.

## PRIORITIZE

Effectively prioritize your exposures based on an AI predictive model with active adversary context. Leverage additional tools and information such as attack path visualization, asset criticality and internet exposure identification to zoom in on the exposures that truly matter to your particular organization.

**ExPRT.AI Ratings**
Automatically prioritize risks with this dynamic AI model trained on CrowdStrike's exploit intelligence and real-life detection events. While CVSS scores categorize many CVEs into high-severity brackets — and inundate resource-strapped security teams — the threat-based ExPRT.AI rating narrows down crucial vulnerabilities to a more targeted set so you can confidently prioritize for more impact with less work.

**Active Adversary Context**
Leveraging industry-leading threat intelligence, Falcon Exposure Management pinpoints and correlates vulnerabilities with adversaries most associated with them and their related tactics so you can better prepare for the types of threats and adversaries that matter most for your particular industry and vertical.

**Attack Path Visualization**
Visualize intrusion risk across endpoint, cloud and identity assets. Understand lateral movement through critical hosts and user accounts. See exactly how an attacker could potentially navigate their way to your organization's crown jewels. With network relationship and risk exposure highlighted, you gain additional information to evaluate whether a particular risk exposure is an isolated risk or a must-fix.

**Asset Criticality**
Asset context is an important consideration for advanced prioritization to further optimize limited resources. The powerful rules engine allows you to automatically assign criticality levels to assets based on a wide variety of input parameters so you know which assets to focus on.

**Internet Exposure Identification**
Not only does Falcon Exposure Management provide an outside-in view of internet-facing IPs, that information is actively correlated against an inside-out view of asset inventory to match and identify exactly which IT assets have an internet exposure. This additional context provides security teams with invaluable information to triage and prioritize risk mitigation.

## REMEDIATE

Whether you are trying to orchestrate remediation activities across the organization or deploy immediate mitigating measures, Falcon Exposure Management has you covered, through integration with both native and third-party tools, powerful platform-based actions and the ability to correlate with CrowdStrike's Falcon Insight XDR solution.

**Native Security Orchestration Automation and Response (SOAR) Integration**
Automate and orchestrate remediation playbooks through CrowdStrike Falcon® Fusion, the SOAR tool built into the Falcon platform. Customize and flexibly trigger ticket assignments to the right teams based on the right remediation actions.

**Third-Party Integrations**
Leverage popular ticketing tools such as ServiceNow and Jira to seamlessly create tickets. The powerful two-way integration allows you to actively monitor the status and track the completion of tasks. Additional integration with remediation and patch management tools adds further convenience and flexibility.

Falcon Real Time Response (RTR) Actions
CrowdStrike's proprietary Falcon RTR actions deliver a powerful range of mitigation measures and compensating controls such as:

- **Compute:**

Kill running process, block file execution, execute patchless config scripts

- **Network:**

Close ports, restrict IP, restrict DNS, restrict network storage

- **Identity:**

Restrict accounts, suspend logins

- **Hardware:**

Restrict USB devices, restrict Bluetooth

**Emergency Patching**
The Falcon RTR-powered emergency patching capability provides one-click patching convenience for Windows-based systems, delivering surgically targeted, precise, proactive protection.

# 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.

# SERVICE ENGAGEMENT

## ORDERING AND INVOICING

The service can be purchased by contacting CrowdStrike: ukpublicsector@crowdstrike.com

Once a contract has been signed and returned to CrowdStrike, the service will be provisioned in line with the agreed terms. In particular, the Call Off Contract will need to list: a minimum non-cancellable subscription term; that the Service Deliverables consist solely of CrowdStrike proprietary Products which are not deemed to be open source or licensed for anyone other than Buyer's use for its own internal information security purposes; an accurate description of the locations where the service is performed (including remote access outside the EEA) and use of our affiliates and listed sub processors; an accurate description of how we process a Buyer's data (I.e. the nature of the data and purposes of processing). Including CrowdStrike's crowd sourcing model (see Exhibit A, Section 2 of the CrowdStrike Terms and Conditions). Invoicing will be undertaken in line with the Order Form and the accompanying Call Off Contract.

Invoicing is annual up-front, with a minimum 12-month term.

## PRICING OVERVIEW

Please refer to the pricing document published alongside this Service Definition.

## ON-BOARDING AND OFF-BOARDING

On-Boarding-

In general, CrowdStrike will complete the following tasks to setup the Cloud Service:

1. Activate the Services as detailed on the Order Form;
2. Provide Service access to the Customer;
3. Provide Professional Services to assist you with on-boarding to the system as described in a SOW or as otherwise mutually agreed in accordance with the order and the Agreement. Please see the CrowdStrike services G-Cloud listing for further details.

Off-Boarding-

Prior to termination, and upon providing 30-days written notice, the Customer shall have the right to access and download Customer Data available per the Customer's purchased Products and data retention period in a manner and in a format supported by the Products.

Please discuss in further detail with CrowdStrike if a bespoke exit plan is required.

## TRAINING

CrowdStrike offers training and certification services to customers, partners, and employees on CrowdStrike technologies and cybersecurity topics to facilitate the adoption of CrowdStrike and to broaden and deepen their skills.

Training is available through CrowdStrike University. CrowdStrike University is an online learning management system (LMS) that organizes all CrowdStrike eLearning, instructor-led training and certification in one place, providing a personalized learning experience for individuals who have an active training subscription.

A CrowdStrike University per-learner training subscription provides fundamental cybersecurity and CrowdStrike Falcon training through self-paced eLearning courses, product update videos, the global training calendar and the online portal for taking CrowdStrike certification exams.

Robust product documentation as well as access to our support portal and knowledge base can be found in the product UI at no cost. Advanced-level training classes require two training credits and a valid annual access pass.

https://www.crowdstrike.com/endpoint-security-products/crowdstrike-university/

## IMPLEMENTATION PLAN

An implementation plan can be provided to the buyer on request and will be included within an agreed Statement of Work (SOW) to be agreed between the parties.

## SERVICE CONSTRAINTS

The CrowdStrike platform is a 27x7x365 platform, as such all maintenance on the platform is performed without customer interruption. Support hours are also persistent, although response times vary based on issue severity.

The platform configuration is highly configurable and customisable. Information about this can be provided in the form of documentation to interested parties.

## SUPPORT AND SERVICE LEVELS

CrowdStrike offers support services to assist with deployment and ongoing use of our products to ensure your success in "stopping the breach." The CrowdStrike support organization is dedicated to resolving issues quickly and effectively. We provide multiple levels of support, so customers can choose the level that best fits their business requirements and ensure they receive the most from their investment in CrowdStrike. CrowdStrike provides four levels of support:

- **Standard.** Bundled free with the Falcon platform, Standard Support includes email communications, access to the support portal, and standard troubleshooting and technical assistance.
- **Express.** Express Support is designed for customers in small to medium-sized enterprise environments where deployment and operational issues must be addressed as quickly as possible.
- **Essential.** Essential Support provides enhanced capabilities to ensure that deployment, operational and management issues are resolved as quickly as possible. It includes extended coverage hours and direct engagement with technical account managers (TAMs).
- **Elite.** Customers with our highest support level, Elite Support, are assigned a dedicated technical account manager to work closely with them as a trusted advisor, proactively providing guidance on best practices to ensure effective implementation, operation and management of the Falcon platform.

For details, visit this link: https://www.crowdstrike.com/endpoint-security-products/crowdstrike-support/.

## AVAILABILITY SLA

CrowdStrike Falcon is a cloud-based solution and CrowdStrike uses commercially reasonable efforts to make the Falcon Platform available at least 99.9% of the time, excluding scheduled downtime for routine maintenance (not to exceed 4 hours a month) and downtime attributable to force majeure (the "Availability SLA"). Compliance with the Availability SLA is measured on a calendar month basis.

The SLA is subject to additional terms which will be agreed and included in the Call Off Contract

# SERVICE PROVISION

## CUSTOMER RESPONSIBILITIES

The customer's obligations are outlined within the CrowdStrike Terms & Conditions, including (without limitation) (i) the usage parameters, and any other terms related to permitted access and use of the Offering (including in relation to Internal Use and Competitors); (ii) ownership terms; (iii) "Compliance with Laws" and US export terms; (iv) CrowdStrike's processing of the Buyer's data as instructed by Buyer and described in Exhibit A to the CrowdStrike Terms and Conditions and related DPA

## TECHNICAL REQUIREMENTS AND CLIENT-SIDE REQUIREMENTS

CrowdStrike provides a lightweight agent, which consumes minimal resources on any supported operating system. As supported systems change with some frequency details are best provided to the interested by contacting CrowdStrike directly.

## AFTER-SALES ACCOUNT MANAGEMENT

CrowdStrike has a Technical Account Management function dedicated to maintaining the technical relationship of our customers. Their interaction, for example but not limited to, include on-site visits, health checks, roadmap webinars. CrowdStrike also has a Client Advisory Program where a dedicated person manages the post-sale relationship and drives the continued success of our customer base.

## TERMINATION

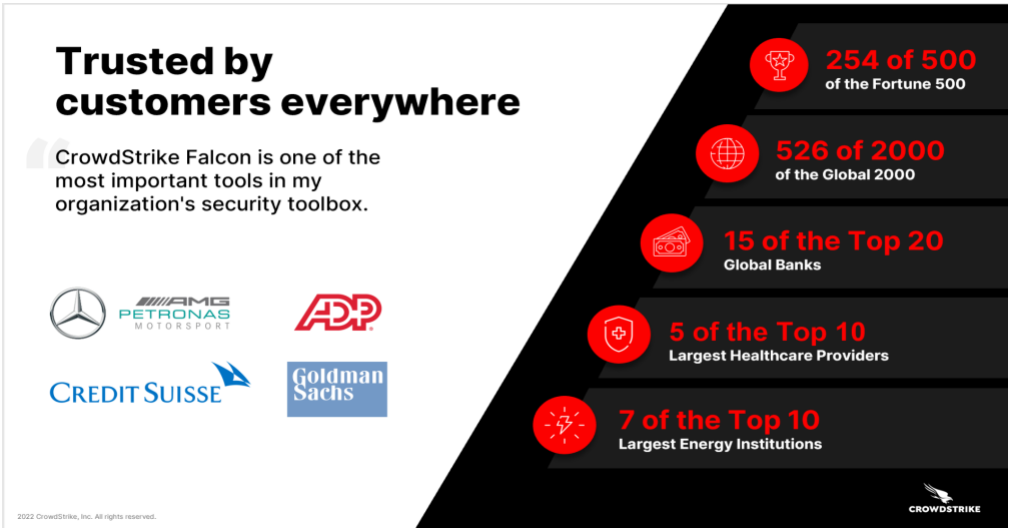
Please see Section 13 of the accompanying CrowdStrike Terms & Conditions and note that pricing is subject to a minimum noncancellable subscription term

# OUR EXPERIENCE

## CASE STUDIES.

CrowdStrike is on a mission to keep customers safe from breaches. Every organization faces unique threats and risk levels that depend on the value their data holds for adversaries. Small companies with limited resources are often tasked with greater security challenges, and larger organizations must deal with vast security considerations on all fronts.

CrowdStrike is fortunate to have customers that are CrowdStrike Champions — watch as they tell stories of how they use the CrowdStrike Falcon platform in creative ways to meet the security challenges of today and stand fully prepared to defend against tomorrow's adversaries.




It's no accident that organizations with some of the most demanding security requirements in the world have turned to CrowdStrike to provide the strongest level of defense against today's sophisticated attacks.

Watch our customer video testimonials at https://www.crowdstrike.com/resources/case-studies/.

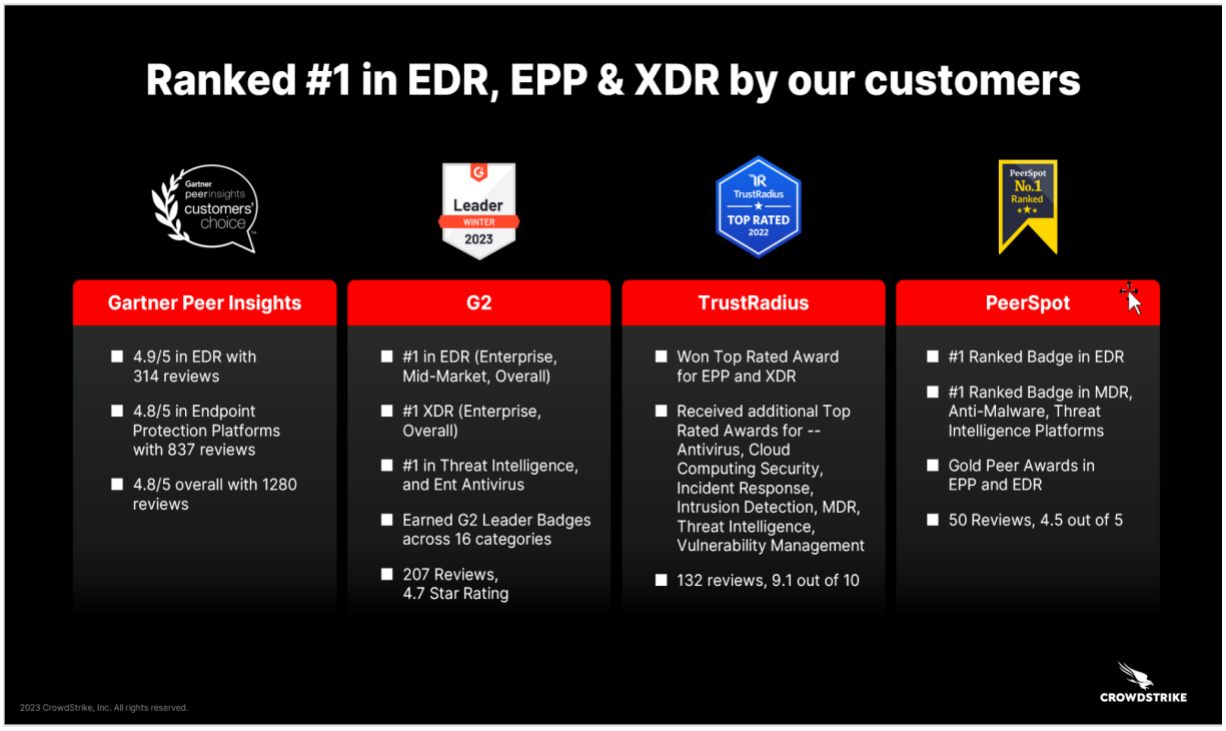
See more verified customer peer reviews at Gartner Peer Insights for Endpoint Detection and Response and for Endpoint Protection Platforms.

## AWARDS AND ACOLADES

The CrowdStrike Falcon platform has become the industry's leading endpoint protection solution, and this has been consistently validated by industry analysts, independent testing organizations and security professionals. If you're looking for a solution that has been tried, tested and proven, then the Falcon platform is for you. You can find out more about CrowdStrike's industry validation here: https://www.crowdstrike.com/why-crowdstrike/crowdstrike-industry-validation/.

Here are some of the industry analysts that have recognized CrowdStrike as a cybersecurity industry leader:

- 2023 Gartner® Magic Quadrant™ for Endpoint Protection Platforms - Nov 2023
- IDC Worldwide Modern Endpoint Security Market Share Report, July 2021-June 2022
- Forrester Wave™: Endpoint Detection and Response Providers, Q4 2023
- Forrester Wave: Cybersecurity Incident Response (IR) Services, Q1 2022




On a company level, CrowdStrike has received the following recognition:

- Named by Fortune Magazine as one of the 2022 Best Workplaces for Women: https://www.crowdstrike.com/press-releases/crowdstrike-named-one-of-the-best-workplaces-for-women/.

- Named to the 2023 Fortune 100 Best Companies to Work For® list for the third consecutive year: https://www.crowdstrike.com/press-releases/crowdstrike-named-to-fortunes-100-best-companies-list-for-third-consecutive-year/.
- Received a perfect score in the Human Rights Campaign Foundation's Corporate Equality Index for the second consecutive year in 2022: https://www.crowdstrike.com/press-releases/crowdstrike-lands-perfect-score-in-hrc-foundations-corporate-equality-index/.

# CONTACT DETAILS

For further details about CrowdStrike please contact email us at: ukpublicsector@crowdstrike.com