FALCON IDENTITY PROTECTION

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 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.

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.

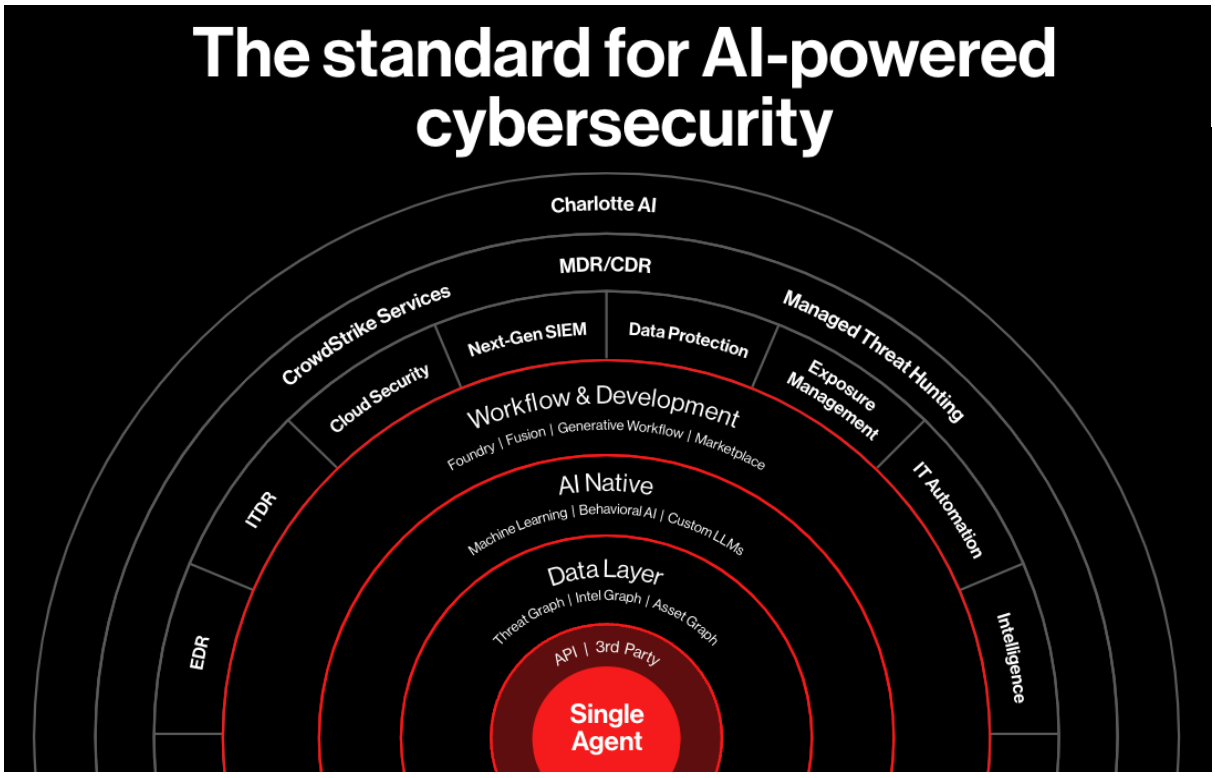
Infused with AI expertise

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.

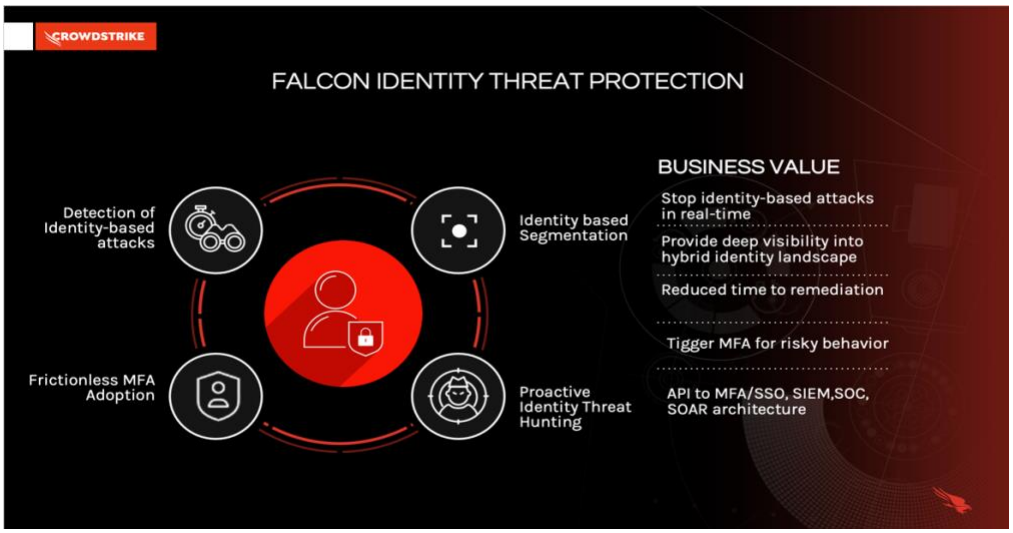
Effortless workflows and automation

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 IDENTITY THREAT PROTECTION



Falcon Identity Threat Protection — fully integrated with the CrowdStrike Falcon platform — is the ONLY solution in the market to ensure comprehensive protection against identity-based attacks in real time. It is part of an overall Zero Trust strategy that covers endpoints, identities, cloud workloads and data.

Falcon Identity Threat Protection enables frictionless Zero Trust security with real-time threat prevention and IT policy enforcement using identity, behavioral and risk analytics. Because 80% of breaches involve compromised credentials, segmenting identities, automating enforcement and using risk-based conditional access to verify authentication traffic can reduce both risk and IT complexity.

SEGMENT - AUTOMATE PROTECTION - VERIFY

Continuous Multi-directory Visibility. Get deeper visibility into the scope and impact of access privileges for identities across Microsoft Active Directory, Azure AD and cloud SSO solutions. Automatically classify identities into hybrid (identities that are on on-premises and cloud AD) and cloud-only (identities that reside only on Azure AD), and segment accounts into human, service/programmatic, shared accounts and privileged accounts across hybrid identity stores.

Customizable Security Posture Overview. See the attack path. Analyze user risk and behavior changes over time — like increase in account lockouts, high-risk endpoints and compromised passwords — to get an overview of the risk posture of the organization.

Hybrid Identity Store Protection. Continuously analyze every account across on-premises and hybrid identity stores. Inspect live authentication traffic, including encrypted protocols (e.g., LDAP/S).

Log-free, Real-time Threat Detection. Continuously assess security and incidents around identity threats without requiring the ingestion of logs or complex analysis. Powered by the world's largest unified, threat-centric data fabric, uncover reconnaissance (e.g., LDAP, BloodHound, SharpHound, credential scanning),

lateral movement (e.g., RDP, Mimikatz tool, unusual endpoint usage, unusual service logins), and persistence (e.g., Golden Ticket attack, hidden objects, privilege escalations) with increased accuracy. Logs (from SIEM, VPN, etc.) can always be provided for additional context but are not required for detecting identity threats.

Intuitive Threat Hunting. Investigate faster with unified visibility into accounts across hybrid identity stores without the need for complex, string-based queries. Choose from a list of predefined search criteria (e.g., authentication events, unencrypted protocols, user roles, IP reputation, risk scores), or create your own search criteria to proactively sift through raw events and email them as periodic reports.

Frictionless Identity Verification with Flexible Policies. Define and enforce policies with multiple rules based on authentication patterns, behavior baselines and individual risk scores to verify identities. Use multifactor authentication (MFA) to secure access to identity stores and applications, and improve the user experience (i.e., identity verification is triggered only when the risk increases or if there's a deviation from normal behavior).

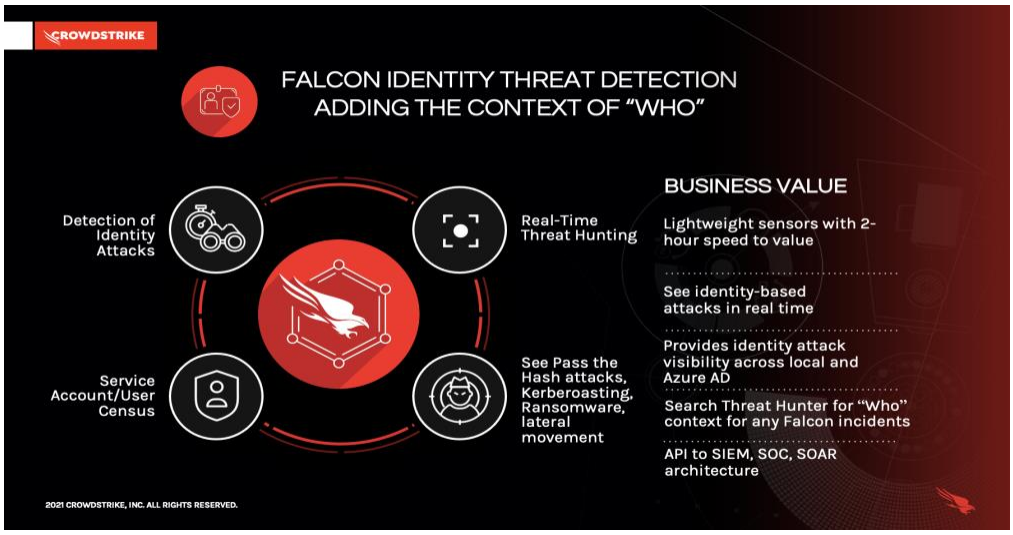
Improved Security Posture and Coverage with Extended MFA. Extend identity verification/MFA to any resource or application, including legacy/proprietary systems and tools (e.g., desktops that are not covered by cloud-based MFA solutions, and on tools like PowerShell and protocols like RDP over NTLM) and reduce the attack surface. Extend the platform's risk score and high-fidelity information with minimal effort to other apps using API-based connectors.

KEY BENEFITS OF IDENTITY THREAT PROTECTION:

- Realize value from Day One — gain unified visibility and security control of access to applications, resources and identity stores in hybrid environments.
- Reduce mean time to detect and respond and improve SOC analysts' efficiency and response times by collating all connected anomalies and alerts into incidents.
- Improve alert fidelity and reduce noise by recognizing and auto-resolving genuine access incidents with identity verification.
- Enforce consistent risk-based policies with zero friction — actions include block, allow, audit, reset password and step-up using MFA.
- Save log storage costs by storing only relevant authentication logs.
- Increase ROI from your MFA investment by extending it to legacy applications and tools.

Product page:
https://www.crowdstrike.com/resources/data-sheets/falcon-complete-identity-threat-protection/

FALCON IDENTITY THREAT DETECTION



Falcon Identity Threat Detection is a CrowdStrike Falcon Identity Protection module that offers a subset of focused features (detection-only) of the Falcon Identity Threat Protection product.

Falcon Identity Threat Detection offers complete visibility and risk scores for all credentials — on-premises or in the cloud — and monitors authentication traffic in both directions to identify anomalies and attacks without additional agents on the endpoint or application servers. Because 80% of breaches involve compromised credentials, alerting on these attacks as they occur identifies compromised assets and credentials in real time.

Active Directory Security Posture and Hygiene. See all credentials in the organization — both on-premises and in the cloud — in one location, with analysis on compromised passwords, privileges, type (service/programmatic vs human user), with user profiles providing individual and group risk scores.

See and Detect Identity Attacks Live — Everywhere. See anomalies and identity-based attacks against all users, including anomalies from privileged and remote users, and alert on insider threats in real time without requiring logs or user workflow changes, and with no changes to existing Falcon endpoint agents.

Identify Lateral Movement and Ransomware Proliferation. See all RDP traffic and monitor all authentication locally and in the cloud. Alert on stale accounts and privilege changes and enable incident response with identity chain correlation across all monitored networks. The internal Threat Hunter tool is focused on identity store security, offering incident response and Blue Team visibility for every stage of an attack involving identities.

KEY BENEFITS OF FALCON IDENTITY DETECTION:

- Discover all identities across the enterprise — including stale accounts — with password hygiene.

- Verify identity store (e.g., Active Directory, LDAP/S) security to discover weakness across multiple domains.
- Investigate authentication events and questionable user behavior.
- Group events around user, device, protocol activity and more for improved incident response.
- Gain unified visibility for authentication traffic to applications, resources and identity stores.
- Reduce mean time to detect and respond, and improve SOC analysts' efficiency and response times by cutting down on the need to do complex, error-prone log analysis.
- Improve alert fidelity and reduce noise by recognizing true positive events of interest.

Product page: https://www.crowdstrike.com/resources/data-sheets/falcon-identity-threat-detection/

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

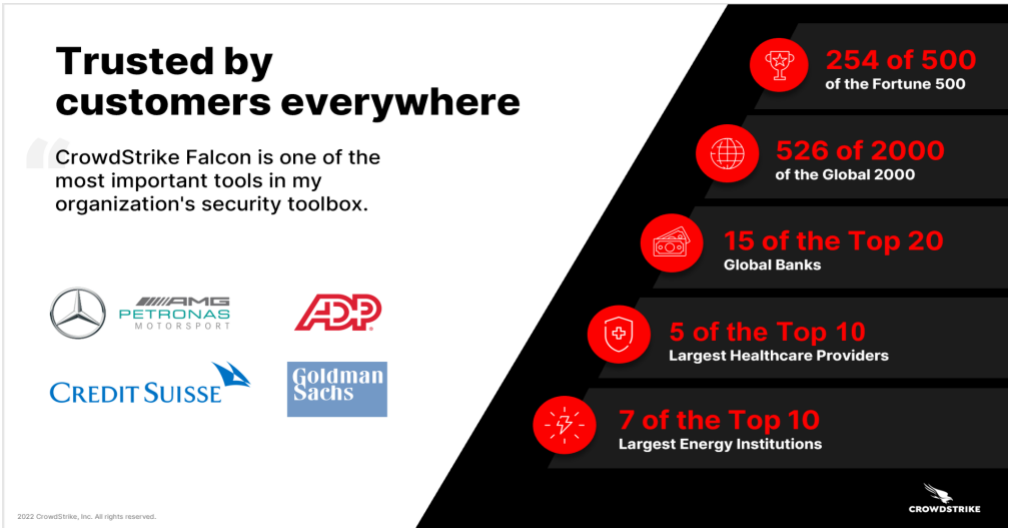
Please see Section 13 of the accompanying CrowdStrike Terms & Conditions and note that pricing is subject to a minimum noncancellable subscription term

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/.

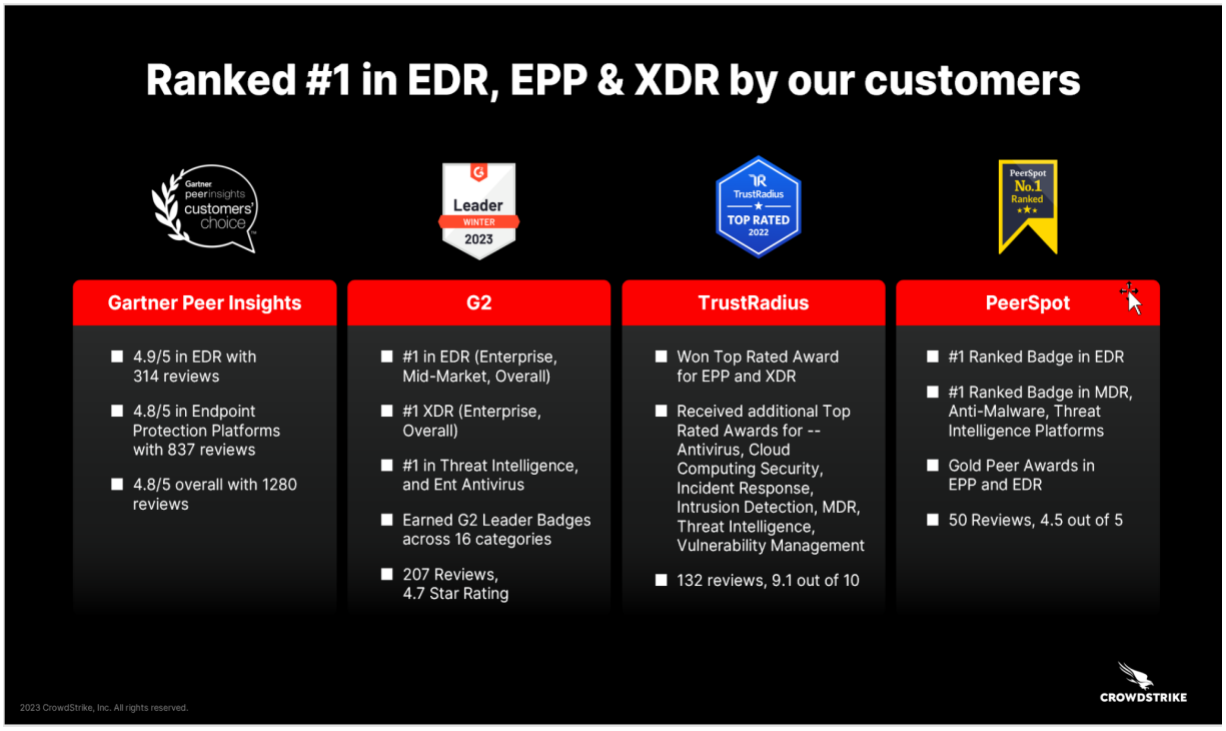
See more verified customer peer reviews at Gartner Peer Insights for Endpoint Detection and Response and for Endpoint Protection Platforms.

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