eSENTIRE

Description:
CrowdStrike License Add-Ons

1. Overview

As an active Endpoint Services - CrowdStrike (the "**Service**") customer of eSentire, Client may order additional CrowdStrike, Inc. ("**Product Publisher**") license entitlements from eSentire, outside of those required or supported by the Service ("**Add-Ons**"). Any such Add-Ons will be provided for Client use, but other than as described below, do not include any eSentire support or configuration assistance. When Client orders the Service from eSentire in an MSSP support model, eSentire is considered the licensee of such Add-Ons (referred to on the Order Form as an "**MSSP Add-on**" or "**Add-on**") and eSentire will provide access and documentation to Client. Client can request assistance with such MSSP Add-ons from eSentire, and eSentire will open a ticket with Product Publisher. When Client orders the Service from eSentire in an Enterprise support model, Client is considered the licensee of such Add-Ons (referred to on the Order Form as an "**Enterprise Resale**" or "**Resale**") and Client will need troubleshoot such components directly with CrowdStrike, Inc. eSentire does not warrant or guarantee the successful operation of Add-Ons. Add-Ons are made available by eSentire to Client on an "as-is" basis and eSentire specifically disclaims all representations and warranties with respect to Add-Ons, express or implied, including the implied warranties of merchantability, operability, and fitness for a particular purpose. Use of any such Add-Ons is subject to Client's acceptance of and compliance with the full Product Publisher EULA which applies to the Add-Ons, which can be found here: www.crowdstrike.com/terms. A description of the Service, and of MSSP and Enterprise support models can be found in the Endpoint Services – Crowdstrike Service Description which can be found under "Managed Detection and Response ("MDR") Services" on this webpage: https://www.esentire.com/legal/documents.

2. Descriptions

A list of available Add-Ons and high-level summaries are as follows (subject to change at Product Publisher's discretion, see data sheet references below for up-to-date descriptions):

2.1 Falcon Cloud Security. CrowdStrike Falcon Cloud Security (FCS) is an optional subscription that provides comprehensive and consistent security for cloud-based environments. It offers workload runtime protection (CWP) and cloud security posture management (CSPM) across AWS, Azure and GCP. FCS integrates agent-based and agentless protection to prevent, detect and respond to cloud breaches and to reduce the risk of misconfigurations and human error in cloud environments. See Product Publisher data sheet for current detailed descriptions located here: https://www.crowdstrike.com/resources/data-sheets/crowdstrike-falcon-cloud-security/.

2.2 Falcon Data Protection. CrowdStrike Falcon Data Protection is an optional subscription that provides real-time visibility and control over sensitive data as it moves from endpoints to USBs or via web browsers to cloud and SaaS applications. It is a Data Loss Prevention (DLP) solution that enables the enforcement of policies to allow, monitor and block classified data movement. Falcon Data Protection is enabled and configured within the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-data-protection/.

2.3 Falcon Data Replicator. CrowdStrike Falcon Data Replicator (FDR) is an optional subscription that provides the option to transform and forward data from the Falcon platform to supported cloud storage mechanisms such as AWS S3 buckets and Google Cloud buckets. This is the default option for

any customer requiring more than 15-days raw telemetry retention or for customers who want to enable third-party access to their data in the future. FDR is enabled and configured within the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-data-replicator/.

2.4 Falcon Device Control. CrowdStrike Falcon Device Control is an optional subscription that provides removable media device control functionality, enabling administrators to define and enforce device control policies that regulate the access and use of USB devices on the endpoints. It also records and reports device usage history, logs and file transfers to and from USB storage devices. Falcon Device Control is enabled and configured within the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-device-control/.

2.5 Falcon Discover. CrowdStrike Falcon Discover is an optional subscription that provides IT hygiene and security operations capabilities within the Falcon platform. It collects and analyzes data about applications, assets, and accounts across the customer's environment and displays it in real-time dashboards and reports. It helps the customer to identify unmanaged or unauthorized entities, track software usage and resource consumption, and maintain audit and compliance obligations. Falcon Discover is enabled and configured within the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-discover/.

2.6 Falcon FileVantage. CrowdStrike Falcon FileVantage is an optional subscription that provides file integrity monitoring (FIM) for visibility and reporting on changes to files, folders and registries across an organization's network. It allows administrators to create and enforce policies and groups to monitor critical system and configuration files, as well as content files, for compliance and security purposes. FileVantage is enabled and configured in the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-filevantage-for-security-operations/.

2.7 Falcon Firewall Management. CrowdStrike Falcon Firewall Management is an optional subscription that provides a host-based firewall. This allows for a centralized interface for creating, modifying enforcing and managing firewall policies. Activities and network events are logged in the platform for faster troubleshooting, auditing and compliance purposes. Falcon Firewall Management is enabled and configured within the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-firewall-management/.

2.8 Falcon Forensics. CrowdStrike Falcon Forensics is an optional subscription that provides forensic data collection and analysis of point-in-time and historical data from endpoints for incident response, compromise assessment, threat hunting and monitoring purposes. Falcon Forensics uses a dissolvable executable that is deployed via Falcon's Real Time Response (remote shell) capability and does not persist on the endpoint, leveraging the Falcon platform for data processing and storage. Falcon Forensics provides users with preset and customizable dashboards, filters and queries to examine forensic artifacts and correlate them with threat intelligence data and enables users to download and export data via Falcon Data Replicator (included for Forensics data only). Falcon Forensics is enabled

and configured within the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-forensics/.

2.9 Falcon for Mobile. CrowdStrike Falcon for Mobile is an optional subscription that provides extends EDR coverage to Android and iOS devices. It leverages the Falcon platform's detection technology and threat intelligence to identify and block malicious and unwanted activity on mobile devices, including phishing, jailbreaking, rooting, OS integrity issues, and other mobile threats. It provides unified visibility and response across all endpoints and respects user privacy by only monitoring designated corporate apps, not personal apps on the device. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-for-mobile/.

2.10 Falcon Sandbox. CrowdStrike Falcon Sandbox is an optional subscription that provides malware detonation and analysis in a secure sandbox environment. It monitors and extracts the behavior and interaction of malicious files, network and memory activity, and provides indicators of compromise (IOCs) and analysis reports. It supports various operating systems and file types and integrates with other security solutions. This subscription allows for up to 500 detonations per month. Falcon Sandbox is enabled and configured within the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-sandbox/.

2.11 Falcon for IT Automation. CrowdStrike Falcon for IT is an optional subscription that provides predefined, scheduled and generative AI queries across endpoints, servers and cloud workloads managed within the Falcon platform. It supports key use cases such as fleet management, compliance, forensic investigations and performance monitoring as well as actions directly on the endpoint with Falcon Real Time Response (RTR) to resolve issues, update policies, modify files or registry keys and run executables. Falcon for IT is enabled and configured within the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/crowdstrike-falcon-for-it/.

2.12 Falcon Spotlight. CrowdStrike Falcon Spotlight is an optional subscription that provides continuous vulnerability assessment, management and prioritization for IT analysts. Falcon Spotlight enables IT staff to automate and optimize vulnerability remediation processes, and to integrate with other Falcon modules for additional security capabilities. Falcon Spotlight is enabled and configured within the Falcon platform and does not require additional hardware or software for endpoints with the Falcon agent installed. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/resources/data-sheets/falcon-spotlight/.

2.13 CrowdStrike University. CrowdStrike University is an optional per-user subscription that is not part of the Falcon platform. Yearly passes can be resold to eSentire customers (including MSP customers). eSentire will not have access to the customer's licenses or be able to provision user access to the LMS platform but can facilitate the exchange with CrowdStrike. Product Publishers data sheet with current description is located here: https://www.crowdstrike.com/crowdstrike-university-training-catalog.pdf.