
Service Description

ArcSight Intelligence for CrowdStrike

July 2021



Contents

Contents	2
Standard Service Features.....	3
Solution Data Backup and Retention	6
SaaS Security	6
Audit	8
Micro Focus Security Policies	8
Security Incident Response	8
Micro Focus Employees and Subcontractors	9
Data Subject Requests	9
Scheduled Maintenance.....	9
Service Decommissioning.....	10
Service Level Commitments	10

“This Service Description describes the components and services included in Micro Focus ArcSight Intelligence for CrowdStrike Software-as-a-Service (which also may be referred to as “SaaS”). Unless otherwise agreed to in writing this Service Description is subject to the Micro Focus Customer Terms for Software-as-a-Service or the applicable Micro Focus Pass-Through Terms and represents the only binding terms governing Micro Focus International plc and its affiliates (“Micro Focus”) respective obligations regarding its provision of this SaaS to the end-user customer. Any other descriptions of the features and functions of the SaaS, public statements, including advertisements, shall not be deemed as additional features or functionalities that Micro Focus is required to deliver.”

Standard Service Features

High Level Summary

ArcSight Intelligence (formerly Intersect) provides a security analytics capability, whereby entities such as user accounts, workstations, and servers, are scored for risk based on the scope and scale of anomalies observed. It uses online unsupervised machine learning, which means that the solution automatically builds baseline data for all behaviors being monitored (aka, models). The actual models that are triggered are determined by the type of data being ingested as well as the data attributes that are present in the data.

The unsupervised machine learning approach is ideally suited to help threat hunters find insider threats and external advanced threats (such as nation-state attacks) that manifest as internal threats. This is because the nature of these types of advanced threats is such that an exhaustive set of examples cannot practically be described. This makes these types of threats impossible to find with supervised machine learning.

SaaS service delivery components

SaaS Delivery Components	
One Production Tenant*	✓
ArcSight Threat Hunting	○
✓ = Included ○	

The ArcSight Intelligence for CrowdStrike SaaS offering is provisioned using a single Tenant within a multi-tenant environment. Each customer has their data logically and securely segregated in such an architecture. Each customer is called a tenant.

ArcSight Threat Hunting

The Threat Hunting Service for this offering is designed to maximize the value obtained from the solution, by minimizing the amount of time to detect potentially malicious activity and maximize the opportunity to catch malicious activity before a breach occurs.

Threat hunting resources are difficult to attract and retain. This service allows organizations to extend their capacity without committing to permanent headcount increases.

ArcSight Threat Hunting	
Daily threat hunting in your CrowdStrike data	✓
Weekly reports and optional meeting to review activities that were found	✓

Critical escalation for urgent issues discovered while threat hunting



✓ = Included

SaaS operational services

Operational Services

Welcome Pack



Help Desk Support



✓ = Included

Architecture Components

The ArcSight Intelligence for CrowdStrike Offering is a SaaS-based analytics engine that consumes CrowdStrike EDR events, analyses those events for risky, unusual behaviors, and provides daily results back. The CrowdStrike application periodically sends data to the ArcSight Intelligence for CrowdStrike analytic engine for analysis via API integration, and analytical results are published daily via the ArcSight Intelligence UI for exploration.

The ArcSight Intelligence for CrowdStrike is a multi-tenant environment, meaning that each customer receives their own unique tenant. This tenant segregates their analyses and underlying data from all other tenants.

Application Administration

All data provided to the ArcSight Intelligence for CrowdStrike will be considered Customer-provided SaaS Data per the Micro Focus Customer SaaS Terms. CrowdStrike is responsible for all data collection and data accuracy as part of any assessment request. Micro Focus is not responsible for the accuracy of the data provided by CrowdStrike. The import of Customer data into the ArcSight Intelligence for CrowdStrike solution requires that the information is made available to Micro Focus at the appropriate step of the ArcSight Intelligence for CrowdStrike solution and in the agreed-to format. The analysis will be performed remotely and delivered in English only.

Analytical Results Delivery

The ArcSight Intelligence for CrowdStrike application performs its analysis once a day at a different time for each tenant. These results include:

- entity risk scores
- anomalous events
- descriptions and visualizations for anomalous events

Service Support

The Customer may contact Micro Focus through the CyberResSupport@microfocus.com or access CyberRes Portal at <https://support.cyberreshelp.com> . The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support. The severity of the request determines the response from the team.

Severity Level	Technical response	Update Frequency	Target For Resolution	What Qualifies?
1	Immediate	Hourly	4 hours	Total or substantial failure of service. Known or suspected security events
2	30 mins	Every 2 hours	8 hours	Significant degradation of service, major feature inability
3	4 hours	Every 8 hours	24 hours	Performance issues outside the of the norm but not substantial enough to prevent usability of a feature. Issues with reports generated from within the customer's Tenant
4	As available	As available	Determined by the customer impact or LOE	Bugs in deployed products not substantial enough to prevent required customer functionality from being accessible but requiring development time to resolve.

Service Monitoring

Micro Focus monitors ArcSight Intelligence for CrowdStrike solution components for 24x7 availability. Micro Focus uses a centralized notification system to deliver proactive communications about application changes, outages and scheduled maintenance.

Capacity and Performance Management

The ArcSight Intelligence for CrowdStrike SaaS environment is continually monitored for performance issues. Proactive capacity and performance management procedures are in place to ensure the architecture of the environment meets the needs of its customers. The architecture allows for addition of capacity to applications, databases and storage.

Operational Change Management

Micro Focus follows a set of standardized methodologies and procedures for efficient and prompt handling of changes to SaaS infrastructure and application, which enables beneficial changes to be made with minimal disruption to the service. Changes to production environments are reviewed prior to implementation to ensure they are appropriately scheduled and tested before promotion to production.

Solution Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus's overall business continuity management practices designed to attempt to recover availability to Customer of ArcSight Intelligence for CrowdStrike application and access to the ArcSight Intelligence for CrowdStrike application, following an outage or similar loss of service.

The Data Backup Frequency is one (1) day and Micro Focus performs that daily backup of the ArcSight Intelligence for CrowdStrike tenant metadata and configuration data, event data and analytical results. The Backup Retention Time is thirty (30) days, meaning Micro Focus retains each daily backup for the most recent thirty (30) days ("Data Retention Time").

Micro Focus's standard storage and backup measures are Micro Focus's only responsibility regarding the retention of this data, despite any assistance or efforts provided by Micro Focus to recover or restore Customer's data.

Disaster Recovery

1. Business Continuity Plan

Micro Focus SaaS continuously evaluates different risks that might affect the integrity and availability of Micro Focus SaaS. As part of this continuous evaluation, Micro Focus SaaS develops policies, standards and processes that are implemented to reduce the probability of a continuous service disruption. Micro Focus documents its processes in a business continuity plan ("BCP") which includes a disaster recovery plan ("DRP"). Micro Focus utilizes the BCP to provide core Micro Focus SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that Micro Focus SaaS implements and tests Micro Focus SaaS recovery capabilities to reduce the probability of a continuous service interruption in the event of a service disruption.

2. Backups

Micro Focus SaaS utilizes cloud-native functions such as replication between primary and secondary availability zones to ensure data availability and recoverability. All replicas reside within the same governmental compliance boundary to ensure adherence to all applicable data residency regulations. Real-time replication is used between primary and standby nodes to facilitate an RPO of 2 hours (Real-time replication is used between nodes). No removable media is used at any time to ensure the protection of customer data.

SaaS Security

Micro Focus maintains an information and physical security program designed to protect the confidentiality, availability and integrity of Customer Personal Data and confidential information (the "Micro Focus Security Program").

Technical and Organizational Measures

This section describes Micro Focus's standard technical and organizational measures, controls and procedures, which are intended to help protect the Customer-provided SaaS Data. Micro Focus regularly tests and monitors the effectiveness of its controls and procedures. No security measures are or can be completely effective against all security threats, present and future, known and unknown. The measures set forth in this section may be

modified by Micro Focus, but represent a minimum standard. Customer remains responsible for determining the sufficiency of these measures.

Physical Access Controls

Micro Focus maintains physical security standards designed to prohibit unauthorized physical access to the Micro Focus equipment and facilities used to provide SaaS and include Micro Focus data centers and data centers operated by third parties. This is accomplished through the following practices:

- presence of on-site security personnel on a 24x7 basis;
- use of intrusion detection systems;
- use of video cameras on access points and along perimeter;
- Micro Focus employees, subcontractors and authorized visitors are issued identification cards that must be worn while on premises;
- monitoring access to Micro Focus facilities, including restricted areas and equipment within facilities; securing equipment hosting Customer-provided SaaS Data in designated caged areas; and maintaining an audit trail of access.

Access Controls

Micro Focus maintains the following standards for access controls and administration designed to make Customer-provided SaaS Data accessible only by authorized Micro Focus personnel who have a legitimate business need for such access:

- secure user identification and authentication protocols;
- authentication of Micro Focus personnel in compliance with Micro Focus standards and in accordance with ISO27001 requirements for segregation of duties
- Customer provided SaaS data is accessible only by authorized Micro Focus personnel who have a legitimate business need for such access, with user authentication, sign-on and access controls;
- employment termination or role change is conducted in a controlled and secured manner;
- administrator accounts should only be used for the purpose of performing administrative activities;
- each account with administrative privileges must be traceable to a uniquely-identifiable individual;
- all access to computers and servers must be authenticated and within the scope of an employee's job function;
- collection of information that can link users to actions in the Micro Focus SaaS environment;
- collection and maintenance of log audits for the application, OS, DB, network and security devices according to the baseline requirements identified;
- restriction of access to log information based on user roles and the "need-to-know;" and prohibition of shared accounts.

Availability Controls

Micro Focus's business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption. Micro Focus's continuity plans cover operational shared infrastructure such as remote access, active directory, DNS services, and mail services. Monitoring systems are designed to generate automatic alerts that notify Micro Focus of events such as a server crash or disconnected network.

Controls regarding disruption prevention include:

- uninterruptible power supplies (UPS) and backup power generators;
- at least two independent power supplies in the building; and
- robust external network connectivity infrastructure.

Data Segregation

Micro Focus SaaS environments are segregated logically by Micro Focus SaaS access control mechanisms. Internet-facing devices are configured with a set of access control lists (ACLs), which are designed to prevent unauthorized access to internal networks. Micro Focus uses security solutions on the perimeter level such as: firewalls, IPS/IDS, proxies and content based inspection in order to detect hostile activity in addition to monitoring the environment's health and availability.

Data Encryption

Micro Focus SaaS uses industry standard techniques to encrypt Customer-provided SaaS Data in transit. All inbound and outbound traffic to the external network is encrypted.

Audit

Micro Focus appoints an independent third party to conduct an annual audit of the applicable policies used by Micro Focus to provide the applicable Micro Focus ArcSight Intelligence for CrowdStrike solution. A summary report or similar documentation will be provided to Customer upon request. Subject to the execution of Micro Focus's standard confidentiality agreement, Micro Focus agrees to respond to a reasonable industry standard information security questionnaire concerning its information and physical security program specific to Micro Focus SaaS provided pursuant to the applicable Supporting Material no more than once per year. Such information security questionnaire will be considered Micro Focus Confidential Information.

Micro Focus Security Policies

Micro Focus conducts annual reviews of its policies around the delivery of SAAS against ISO 27001. Micro Focus regularly re-evaluates and updates its information and physical security program as the industry evolves, new technologies emerge or new threats are identified.

Security Incident Response

In the event Micro Focus confirms a security incident resulted in the loss, unauthorized disclosure or alteration of Customer-provided SaaS Data ("Security Incident"), Micro Focus will notify Customer of the Security Incident and work to mitigate the impact of such Security Incident. Should Customer believe that there has been unauthorized use of Customer's account, credentials, or passwords, Customer must immediately notify Micro Focus Security Operations Center via cyberressuport@microfocus.com.

Micro Focus Employees and Subcontractors

Micro Focus requests that all employees involved in the processing of Customer-provided SaaS Data are authorized personnel with a need to access the Customer-provided SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of customer data. Micro Focus requests that any affiliate or third party subcontractor involved in processing Customer-provided SaaS Data enters into a written agreement with Micro Focus, which includes confidentiality obligations substantially similar to those contained herein and appropriate to the nature of the processing involved.

Data Subject Requests

Micro Focus will, within three (3) business days of receipt, refer to Customer any queries from data subjects in connection with Customer-provided SaaS Data.

Scheduled Maintenance

To enable Customers to plan for scheduled maintenance by Micro Focus, Micro Focus reserves predefined timeframes to be used on an as-needed basis.

A twenty-four-hour period once a quarter starting at Saturday, midnight in the local data center region, and ending on Sunday, midnight.

- This window is considered an optional placeholder for major releases and events that could be significantly service impactful. If the window is to be exercised, and a major disruption expected, all customers should be notified no later than ten business days before.

A two-hour maintenance window once a month starting Wednesday midnight in the local data center region.

- This is for patching of environments. Patching should be done in a non-service disrupting fashion; however, some elements may require a brief outage to update properly. Customers will be notified at least five business days in advance if any actual service disruption is expected.

A four-hour maintenance window once a month starting Saturday, midnight in the local data center region.

- This time is set aside for system updates and product releases that cannot be performed without a visible customer impact. Use of this window is optional, and customers should be notified at least ten business days in advance if any outage is expected.

In case of any holiday conflicts, the regularly scheduled window will automatically fall to the following week on the same day of the week.

Micro Focus determines whether and when to apply a SaaS Upgrade to Customer's Micro Focus ArcSight Intelligence for CrowdStrike SaaS solution. Unless Micro Focus anticipates a service interruption due to a SaaS Upgrade, Micro Focus may implement a SaaS Upgrade at any time without notice to Customer. Micro Focus aims to use the Scheduled Maintenance windows defined herein to apply SaaS Upgrades. Customer may be required to cooperate in achieving a SaaS Upgrade that Micro Focus determines in its discretion is critical for the availability, performance, or security of Micro Focus ArcSight Intelligence for CrowdStrike SaaS.

Service Decommissioning

Customer may cancel Micro Focus SaaS by providing Micro Focus with thirty (30) days written notice prior to the expiration of the SaaS Order Term ("Cancellation"). Such Cancellation shall be effective upon the last day of the then current SaaS Order Term. Upon Cancellation, expiration, or termination of the SaaS Order Term, Micro Focus may disable all Customer access to ArcSight Intelligence for CrowdStrike SaaS solution, and Customer shall promptly return to Micro Focus (or at Micro Focus's request destroy) any Micro Focus Materials.

Micro Focus will make available to Customer such data in the format generally provided by Micro Focus. The target timeframe is set forth below in the Termination Data Retrieval Period SLA section. After such time, Micro Focus shall have no obligation to maintain or provide any such data, which will be deleted in the ordinary course.

Service Level Commitments

Micro Focus provides the following Service Level Commitments for the purpose of further measuring the quality of service that Micro Focus is delivering to the Customer.

1. Solution Provisioning Time SLO

Solution Provisioning is defined as the Micro Focus ArcSight Intelligence for CrowdStrike solution being available for access over the internet. Micro Focus targets to make Micro Focus ArcSight Intelligence for CrowdStrike on SaaS available within five (5) business days of the customer's purchase order (PO) being booked within the Micro Focus order management system.

2. Tenant Off boarding SLO

Micro Focus guarantees a tenant off boarding time of two days from the time in which the Customer submits the formal written request.

3. User Removal SLO

Micro Focus guarantees that after the completion of this request, analytical results about the removed user will no longer be stored or available within the application

4. Analytical Results SLA

Data to analyze is moved from the CrowdStrike Cloud to the ArcSight Intelligence Cloud Service via API. This upload happens continuously, and results in the collection of data within the tenant's storage area (e.g. S3). At a scheduled daily start time, Intelligence will analyze the pending data from a tenant, analyze the collected data, and publish the analytical results back for consumption by the Client, within their assigned tenant.

Micro Focus guarantees that the files in the tenant's daily set events will be analyzed and the results published to the application's user interface before a specified time for each tenant, every 24-hour period, at least 99% of the time.

5. Measurement Method

On a quarterly basis, the availability of the Analytics Results will be measured using the measurable days in the quarter (total days minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator minus the number of days where a tenant's deadline is not met, to give the percentage of days that met the SLA (e.g. 119 days / 120 possible days = 99% availability).

6. Boundaries and Exclusions

The Analytical Results SLA Metric shall not apply in any of the following exceptions, and neither the ArcSight Intelligence for CrowdStrike will be considered unavailable nor any Service Level Failure be deemed to occur in connection with any failure to meet the requirement or impaired ability of Customer or its Authorized Users to access or use the ArcSight Intelligence for CrowdStrike solution:

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Force majeure events as described in the terms of the SaaS agreement
- Actions or omissions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled Maintenance
- Scheduled Version Updates

7. Reporting

Micro Focus will provide Analytical Results SLA Report (“SLA Report”) to the Customer upon request. If the Customer does not agree with the SLA Report, written notice of non-agreement must be provided to Micro Focus within fifteen (15 days) of receipt of the SLA Report

Termination Data Retrieval Period SLO

The Termination Data Retrieval Period is defined as the length of time in which the customer can retrieve a copy of their customer ArcSight Intelligence for CrowdStrike data from Micro Focus. Micro Focus targets to make available such data for download in the ArcSight Intelligence for CrowdStrike format generally provided by Micro Focus for 30 days following the termination of the SaaS Order Term. Standard Service Requirements.

Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to the ArcSight Intelligence for CrowdStrike SaaS solution. Micro Focus’s ability to fulfill its responsibilities relative to SaaS is dependent upon Customer fulfilling the responsibilities described below and elsewhere herein:

Customer Roles and Responsibilities

Customer Role	Responsibilities
Business owner	<ul style="list-style-type: none">• Owns the business relationship between the customer and Micro Focus• Owns the business relationship with the range of departments and organizations using the ArcSight Intelligence for CrowdStrike SaaS solution• Manages contract issues
Subject Matter Expert	<ul style="list-style-type: none">• Leverages & educates other users about the product functionality designed by the ArcSight Intelligence for CrowdStrike SaaS solution

- Provides periodic feedback to the ArcSight Intelligence for CrowdStrike Administrator

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Primary Support Contact (PSC)	<ul style="list-style-type: none"> • Serves as the customer liaison to Micro Focus • Coordinates Micro Focus resources including system and process experts as necessary as well as day to day issues with the SOC staff • Facilitates ongoing mentoring • Coordinates with the customer during required and periodic maintenance • Oversees the customer onboarding process
Service Operation Staff (SOC)	<ul style="list-style-type: none"> • Primary point of contact for service requests. • The Service Operations Center staff is responsible for all services such as support and maintenance, or issues regarding availability of the ArcSight Intelligence for CrowdStrike SaaS solution • Provides 24x7 application support
Operations staff (Ops)	<ul style="list-style-type: none"> • Monitors the ArcSight Intelligence for CrowdStrike SaaS solution for availability • Provides 24x7 SaaS infrastructure and application support • Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus’s standard practices

Assumptions and Dependencies

This Service Description is based upon the following assumptions and dependencies between the Customer and Micro Focus:

- Customer must have internet connectivity to access this Micro Focus ArcSight Intelligence for CrowdStrike SaaS Service.
- Micro Focus ArcSight Intelligence for CrowdStrike SaaS Service will be performed remotely and delivered in English only.
- A SaaS Order term is valid for a single application deployment, which cannot be changed during the SaaS Order term.
- The service commencement date is the date on which Customer’s purchase order (PO) is booked within the Micro Focus order management system.

- The import of Customer data into the ArcSight Intelligence for CrowdStrike SaaS solution during the implementation requires that the information is made available to Micro Focus at the appropriate step of the solution implementation and in the Micro Focus designated format.
- Customer must ensure that its administrators maintain accurate contact information with Micro Focus SaaS.
- Customer has determined, selected, and will use options in the Customer environment that are appropriate to meet its requirements, including information security controls, connectivity options, and business continuity, backup and archival options.
- Customer will establish and follow secure practices for individual account-based access for accountability and traceability.

Furthermore this Micro Focus ArcSight Intelligence for CrowdStrike Service is provided based on the assumption that Customer will implement and maintain the following controls in its use of Micro Focus ArcSight Intelligence for CrowdStrike Service:

- Appointing authorized users
- Configuring its Micro Focus ArcSight Intelligence for CrowdStrike Service account to require that end user passwords are sufficiently strong and properly managed
- Procedures for access approvals, modifications and terminations.

Good Faith Cooperation

Customer acknowledges that Micro Focus's ability to perform the Services depends upon Customer's timely performance of its obligations and cooperation, as well as the accuracy and completeness of any information and data provided to Micro Focus. Where this Service Description requires agreement, approval, acceptance, consent or similar action by either party, such action will not be unreasonably delayed or withheld. Customer agrees that to the extent its failure to meet its responsibilities results in a failure or delay by Micro Focus in performing its obligations under this Service Description, Micro Focus will not be liable for such failure or delay.