Service Description

ArcSight SaaS with Real-Time Threat Detection

August 2023

MICRO FOCUS
is now opentext™

Contents

This Service Description describes the components and services included in Micro Focus ArcSight SIEM on a Software-as-a-Service (which also may be referred to as "SaaS") and, unless otherwise agreed to in writing, is subject to the Micro Focus Customer Terms for Software-as-a-Service ("SaaS Terms") found at https://www.microfocus.com/en-us/legal/software-licensing. Capitalized terms used but not defined herein shall have the meanings set forth in the SaaS Terms.

Standard Service Features

High Level Summary

ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) is a real-time correlation and threat alerting system that increases SOC analyst awareness of critical security incidents in their environment. Detect enables SOC analysts to create correlation rules that generate alerts when specific conditions occur within their event logs. ArcSight SIEM with Detect collects device logs by leveraging ArcSight's SmartConnector framework for log collection, routing, and enrichment. Once collected and received into the SaaS environment, Detect's real-time correlation engine parses the individual events for comparison defined correlation rules. Detect provides an easy-to-use rule creation process using a Java console installed on SOC user workstations. Detect both leverages and extends the existing ArcSight SIEM-as-a-Service capabilities, making use of a consolidation event ingestion framework, shared ArcSight Reporting, shared ArcSight Search, and shared ArcSight SOAR deployment.

SaaS Delivery Components

The Real-Time Threat Detection offering is provisioned with all of the components required to deliver a fully functional product/service offering. It is delivered as a single tenant per customer. Each customer has their data securely segregated in such an architecture and each customer is referred to as a tenant.

SaaS Delivery Components	
One Production Instance	✓
One Test / Dev Instance	O
✓ **= Included**	
O **= Optional for a fee**	

SaaS Operational Services

Operational Services	
Welcome Pack	✓
Help Desk Support	✓
Virtual Connector Host Appliance (vCHA, downloadable)	✓
ArcSight Smart Connector Library (downloadable)	✓
ArcSight Management Center (ArcMC, downloadable)	✓
✓ **= Included**	
O **= Optional for a fee**	

Virtual Connector Host Appliance (vCHA)

The Connector Host Appliance (CHA) was originally developed as a hardware appliance to enhance the deployment options available for the broad array of Smart Connectors that are currently available. As part of the ArcSight SIEM as a Service offering, Micro Focus has enhanced the CHA into

a downloadable Open Virtualized Appliance (OVA) which can be imported into VMware vCenter for easy virtual deployment. This enables on-premise log collection which is then fed to the SaaS environment for search, hunt, and retention availability.

ArcSight Smart Connectors
ArcSight uses smart connectors within the environment. Configuration changes can be made to include an additional destination for the data sources in question. The destination will be a web accessible storage location that is available via the Cloud instance of the ArcSight SIEM as a Service tenant that has been made available. With ArcSight Smart Connectors v8.2 and higher, an export directly to S3, is made available. This method requires a credential to be set during installation. This credential has to have a persistent AWS ID/Key with the correct role.

Once the data sources are identified and set up to be collected by ArcSight SIEM as a Service, and a secure connection has been established data ingest into ArcSight SIEM as a Service can begin.

ArcSight Management Center, (ArcMC) is also available for download for the purpose of managing the Smart Connectors, if desired.

All usage of downloaded components, CHA, Smart Connectors and ArcMC, are to be used ONLY for the purpose of populating ArcSight SaaS services with the customers data and are subject to termination in accordance with the ArcSight SaaS subscription service.

Architecture Components

Detect includes both a web-based and desktop user interface. The web-based interface is used for most day-to-day activities including viewing and searching for events and correlation alerts, creating, and executing reports, and viewing dashboards such as the MITRE dashboard. The desktop application, known as the Java console, is used for both administrative and management tasks, including rule and filter creation.

Micro Focus does not install, deploy, or manage on-premise components that may be required to use Detect.

Service Support
Customers are responsible for some aspects of Application Administration, such as filter, list, and rule creation, user rights limitations, and permissions. Those tasks are primarily performed using the aforementioned Java console. For all other concerns, the Customer may contact Micro Focus through the CyberResSupport@microfocus.com,access CyberRes Portal at https://support.cyberreshelp.com, or call 1(855)982-2261. 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 components of ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) 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
ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) will be 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.

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.

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 SaaS and C SaaS Data for Customer following an outage or similar loss of service for SaaS.

SaaS Data

The following types of SaaS Data reside in the SaaS environment:

- Event data as received from the ArcSight SmartConnector framework
- Correlation Alerts generated by Detect
- Active List and Session List configuration and data
- Correlation Rules
- Customer-created Reports
- Customer-created Saved Searches

- Configuration data including users allowed to log in to the SaaS environment and their preferences

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 for SaaS

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.

Backups (High Availability and Durability)
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 SaaS Data.

Technical and Organizational Measures

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 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 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
- 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"
- Prohibition of shared accounts.
- Use of multi-factor authentication to provide state-of-the-art access to the SaaS systems

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.

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 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 SaaS. A summary report or similar documentation will be provided to Customer upon request. Subject to Customer's 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 SaaS 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, which includes controls derived from ISO 27034 – "Information Technology – Security Techniques – Application Security." 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 SaaS Data ("Security Incident"), Micro Focus will notify Customer of the Security Incident and work to reasonably 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 cyberressec@microfocus.com.

Micro Focus Employees and Subcontractors

Micro Focus requests that all employees involved in the processing of SaaS Data are authorized personnel with a need to access the 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 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 refer to Customer any queries from data subjects in connection with 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 used, 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 SIEM-as-a-Service with Real-Time Threat Detection (Detect)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 <INSERT SOFTWARE NAME HERE> SaaS.

Service Decommissioning

Upon expiration or termination of the SaaS Order Term, Micro Focus may disable all Customer access to SaaS, 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 Termination Data Retrieval Period SLO. 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 Objectives

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.

Solution Provisioning Time Service Level Objective (SLO)

Solution Provisioning is defined as the Micro Focus ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) solution being available for access over the internet. Micro Focus targets

to make Micro Focus ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) available within five (5) business days of the customer's Order being booked within the Micro Focus order management system.

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.

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

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 Micro Focus ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) data from Micro Focus. Micro Focus targets to make available such data for download in the ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) format generally provided by Micro Focus for 30 days following the termination of the SaaS Order Term.

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.

SaaS Availability Service Level Agreement (SLA)
SaaS availability is the SaaS production application being available for access and use by Customer over the Internet. Micro Focus will provide Customer access to the SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.5 % ("Target Service Availability" or "TSA").

Measurement Method
TSA shall be measured by Micro Focus using Micro Focus monitoring software running from a minimum of four global locations with staggered timing. On a quarterly basis, the TSA will be measured using the measurable hours in the quarter (total time minus Downtime Exclusions) as the denominator. The numerator is the denominator value minus the time of any outages in the quarter (duration of all outages combined) to give the percentage of available uptime (2,198 actual hours available / 2,200 possible available hours = 99.9 availability).

An "outage" is defined as two consecutive monitor failures within a five-minute period, lasting until the condition has cleared.

Downtime Exclusions
The TSA shall not apply to or include any time during which SaaS is unavailable in connection with any of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
- Outages caused by disruptions attributable to force majeure events (i.e., unforeseeable events outside of Micro Focus' reasonable control and unavoidable even by the exercise of reasonable care
- Customer-caused outages or disruptions

- Outages not caused by Micro Focus or not within the control of Micro Focus (i.e., unavailability due to problems with the Internet), unless caused by Micro Focus' service providers
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled maintenance activities
- Scheduled SaaS Upgrades
- Customer exceeding the service restrictions, limitations or parameters listed in this Service Description and/or the Order
- Unavailability due to customizations made to the Micro Focus SaaS which are not validated, reviewed, and approved in writing by both parties
- System downtime requested by Customer
- Suspensions of the Micro Focus SaaS by Micro Focus as a result of Customer's breach of the SaaS Terms

Reporting
Micro Focus will provide an Actual Service Availability Report ("ASA Report") in accordance with this Service Level Commitments section to Customer upon request. If Customer does not agree with the ASA Report, written notice of non-agreement must be provided to Micro Focus within fifteen (15 days) of receipt of the ASA Report.

Remedies for Breach of Service Levels

i. **Sole remedy.** Customer's rights described in this section state Customer's sole and exclusive remedy for any failure by Micro Focus to meet the agreed service levels.

ii. **Escalation.** Quarterly ASA below 98% shall be escalated by both parties to the Vice President (or equivalent),

iii. **Credits.** Subject to the terms herein, Micro Focus will issue a credit reflecting the difference between the measured ASA for a quarter is less than the TSA ("**Remedy Percent**"). For clarity, several example calculations using this formula are illustrated in the table below:

Target Service Availability (TSA)	Actual Service Availability	Result	Remedy Percent
99.5%	99.5%		Not Applicable
99.5%	94.5%	5% missed	5%
99.5%	90.5%	9% missed	9%

Customer must request credits in writing to Micro Focus within ninety (90) days of receipt of the ASA Report resulting in such credit and identify the support requests relating to the period where the SaaS production application was not available for access and use by the Customer over the internet. Micro Focus shall apply the requested credits on a quarterly basis.

Standard Service Requirements

Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to the ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) 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	• Owns the business relationship between the customer and Micro Focus • Owns the business relationship with the range of departments and organizations using the ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) solution and associated components • Manages contract issues
Subject Matter Expert	• Leverages and educates other users about the product functionality designed by the ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) solution • Provides periodic feedback to the ArcSight SIEM-as-a-Service with Real-Time Threat Detection (Detect) Administrator

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Primary Support Contact (PSC)	• 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 Service Operations Center staff • Facilitates ongoing mentoring • Coordinates with the customer during required and periodic maintenance • Oversees the customer onboarding process
Service Operation Center Staff (SOC)	• 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 solution • Provides 24x7 application support

Operations Staff (Ops)	• Monitors the customer instance of the application 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 SaaS
- Customer must provide an endpoint where cyDNA SaaS sends Insights Streaming data to
- SaaS will be delivered remotely 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 Order is booked within the Micro Focus order management system
- The import of Customer data into SaaS 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
- 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

Furthermore, SaaS is provided based on the assumption that Customer will implement and maintain the following controls in its use of SaaS:

- Configuring Customer's browser and other clients to interact with SaaS
- Configuring Customer's network devices to access SaaS
- Appointing authorized users
- Configuring its SaaS 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 provide SaaS and related 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.