Service Description

OpenText™ Core – Adversary Signals

February 2025

V7.4

Contents

This Service Description describes the components and services included in OpenText Core – Adversary Signals (which also may be referred to as “Adversary Signals SaaS” or “SaaS”) and, unless otherwise agreed to in writing, is subject to the Micro Focus Customer – OpenText Core – Adversary Signals Software-as-a-Service (“SaaS Terms”), which are provided upon request. Capitalized terms used but not defined herein shall have the meanings set forth in the SaaS Terms.

Standard Service Features

High Level Summary

Adversary Signals SaaS is a cloud-based enterprise service that provides analytics capabilities to customers and the enables customers to expand review of security risks by analyzing internet signaling for suspicious activity against public IP address ranges that they (1) own or are solely responsible for and (2) have granted permission to onboard into the service.

Analyzing internet signals rather than traditional log file analysis-based detection allows for more timely and tailored detection and requires less effort and resource investment for customers. Efficiency is reached by minimizing false positives thereby focusing on customer specific data as opposed to the generic focus provided by traditional threat intelligence.

Adversary Signals outcomes can be leveraged as a data stream into customers' existing technology and combined with classic SIEM like solutions, to provide log-based analytics.

SaaS Delivery Components

Adversary Signals SaaS Delivery Options	
Adversary Signals SaaS Base Package (mandatory initial purchase) • Shared, multi-tenant environment with data separation • Central delivery from our main Adversary Signals SaaS center of excellence • 100 network IPv4 CIDR ranges max /16 in size • 100 single Ipv4 addresses/hosts • Maximum of 500.000 potential IP addresses across all CIDR ranges • One data retrieval per day (DA01) • Data consumption from the service via secure syslog channel or S3 download • Customer Manager coverage in monthly alignment calls to discuss open topics and feedback	✓
Adversary Signals SaaS Data Acquisition (DA) Options • Increased data retrieval frequency • DA02, two data retrievals per day with instant analytics of retrieved data • DA04, four data retrievals per day with instance analytics of retrieved data	O
Adversary Signals SaaS Add-On Package Options • Add-On for Address Ranges ○ Increased IP address coverage for the existing base tenant by 250,000 potential addresses ○ Requires the same data acquisition option as the base tenant ○ Additional 25 network IPv4 CIDR ranges max. /16 in size • Add-On for Hosts and DNS names	O

○ Additional 250 single Ipv4 addresses/hosts ○ Requires the same data retrieval option as the base SKU for the tenant	
Adversary Signals SaaS Pilot • One (1) to six (6) months of Adversary Signals pilot • 125 network IPv4 CIDR ranges max /16 in size • 350 single IPv4 addresses/hosts • A maximum of 750,000 potential IP addresses (all ranges and hosts combined with their maximum possible address allocation) • Only DA01 is available as the data retrieval option • Secure syslog data stream with Adversary Signals Insights or S3 download of Adversary Signals findings • Email notifications of findings and supported CTI	O
✓ = Included	
O = Optional for a fee	

SaaS Operational Services

Adversary Signals SaaS Operational Services	
Quarterly Retrospective Hunting and Readout (Quarterly readout session including a walkthrough of the most prevalent findings)	✓
Premium Threat Hunting (PTH) Service • Daily time boxed threat hunting exercise based on customers Insights • 1/2/4 hours per day available • 1 hour per day "upgrade" available • Weekly scheduled readout session (30-60 minutes) with customer • Presentation and walk-through findings	O
✓ = Included	
O = Optional for a fee	

An Adversary Signals SaaS subscription includes onboarding a set of public IPv4 ranges and addresses into the service. Public IP ranges can be a maximum of "/16" and must be owned and or rightfully controlled by Customer. Add-on packages of CIDR address ranges are available through an add-on package.

IP address ranges onboarded into the service contribute to the "maximum potential IP addresses" allowed per tenant or add-on. For example, a "/24" network range would add 254 potential IP addresses into the service.

Regional and dedicated deployment options are not available in all areas. Requests can be made to the Account Executive to determine availability.

Customer Onboarding

To onboard IP addresses, Customer gives written consent by completing the Statement of Responsibility, which allows Micro Focus to run analytics against the in-scope public IP address space. By this written confirmation, Customer confirms to be the rightful owner or authorized provider of the IP addresses and that its representative is authorized to implement such analytic measures for their IP address spaces. By this written confirmation, Customer also guarantees to inform Micro Focus of any changes regarding ownership or authorized use of those IP addresses.

As part of Customer onboarding, the Micro Focus onboarding team works with Customer to (1) collect in-scope IP address ranges, (2) define a risk profile, and (3) explore all service options so Customer selects the best fitting option; then Micro Focus provides Customer a quick-start guide to help use the service and consume its results.

Adversary Signals SaaS Pilots are onboarded in the same process.

Service Consumption

Customer consumes service outcomes as an “Insights Data Stream” and can use them on-premises to run further analytics, trigger mitigative actions, or other activities.

Pilots

The Pilot scope and the data retrieval options are available as described above. During the Pilot, Customer has access to the same means of data consumption as a standard subscription.

Architecture Components

To consume data from the service, Customer provides an endpoint where the insights stream service sends analytics results in an encrypted format (“Common Event Format” or “CEF”) feed via Syslog over a TLS connection. Customer may need to make changes to their firewall to receive the Insights feed to the Customer organization platform, i.e. SIEM, SOAR, etc.

Service Support

Customer may contact Micro Focus through submitting online support tickets. The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support.
Online support for SaaS is available at: https://support.cyberreshelp.com.

Emails questions to CyberResSupport@microfocus.com.
Call in: 1(855)982-2261

Micro Focus staffs and maintains a 24x5x52 weeks Service Operations Center with on-call coverage on weekends and holidays for Severity 1 issues, which will be the single point of contact for all issues related to the support for SaaS. Customer will be responsible for maintaining a list of authorized users who may contact Micro Focus for support. Customer’s authorized users may also contact Micro Focus for support via the Web portal or telephone 24 hours a day, 7 days a week.

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 Micro Focus level of effort	Issues 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 SaaS availability 24x7. Micro Focus uses a centralized notification system to deliver proactive communications about service changes, outages and scheduled maintenance. Alerts and notifications are emailed to Customer at customer-provided notification addresses.

Capacity and Performance Management

Application capacity can be increased as required by Customer.

Customers can opt in to a premium threat hunting (PTH) service which helps customer analyst teams to understand findings from our Adversary Signals service and work with them more efficiently.

Customers can choose more frequent than once daily data acquisition and analytics runs of adversary activity signals. Data Acquisition (DA) options are DA01, DA02, and DA04 and refer to the number of data retrievals per day for the full scope of purchased address spaces.

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 to enable beneficial changes to be made with minimal disruption to the service.

Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus' overall business continuity management practices designed to attempt to recover access to SaaS and SaaS Data for Customer following an outage or similar loss of SaaS service.

SaaS Data

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

- Public IPv4 address ranges
- ASN information
  - ASN information describes customers' "internet routing domains" in which their public IP addresses are managed

Micro Focus performs a backup of SaaS Data every day. Micro Focus retains backups for the most recent seven (7) days.

Micro Focus’ standard storage and backup measures are Micro Focus’ only responsibility regarding the retention of this SaaS Data. Customer may request via a service request for Micro Focus to attempt to restore such data from Micro Focus’ most current backup. Micro Focus will be unable to restore any data not properly entered by Customer or lost or corrupted at the time of backup or if Customer´s request comes after the 7-days data retention time of such backup.

For backup and recovery reasons, relevant configuration files are secured in backup locations to enable rapid recovery after failure.

Disaster Recovery for SaaS

Business Continuity Plan
Micro Focus continuously evaluates different risks that might affect the integrity and availability of SaaS. As part of this continuous evaluation, Micro Focus 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 SaaS and infrastructure services with minimum disruption. The DRP includes a set of processes that implements and tests 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. 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.

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 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´ business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption. Micro Focus' 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
- Robust external network connectivity infrastructure

Data Segregation

SaaS environments are segregated logically by 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 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. Subject to Customer's execution of Micro Focus' 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 SED@opentext.com.

Micro Focus Subcontractors

Micro Focus requires 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.

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 significantly impact service. 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.

Scheduled Version Updates

"SaaS Upgrades" are defined as major version updates, minor version updates, and binary patches applied by Micro Focus to Customer's SaaS in production. These may or may not include new features or enhancements. Micro Focus determines whether and when to develop, release and apply any SaaS Upgrade. Customer is entitled to SaaS Upgrades during the applicable Adversary Signals Order Term unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Service Decommissioning

Upon expiration or termination of the Adversary Signals Order Term, Micro Focus may disable all Customer access to SaaS, and Customer shall promptly return to Micro Focus (or at Micro Focus request, destroy) any Micro Focus materials.

Micro Focus will make available to Customer any SaaS Data in Micro Focus' possession 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 clear, detailed, and specific Service Level Objectives (SLOs) for SaaS. These SLOs are targets used by Micro Focus to deliver the service and are provided as guidelines. They in no way create a legal requirement or obligation for Micro Focus to meet these objectives.

Solution Provisioning Time SLO
Solution Provisioning is defined as SaaS being available for access over the internet. Micro Focus targets to make SaaS available within five (5) business days of Customer's submission of Customer's onboarding documentation.

Customer is responsible for installing, configuring, deploying, updating and paying any additional fees (if required) for any additional on-premise components for its applications. Any on-premises components of the solution are not in scope of the Solution Provisioning Time SLO.

Additionally, the import of Customer data into the application is not in scope of the Solution Provisioning Time SLO.

Solution Availability SLO
Solution Availability is defined as the SaaS production application being available for access and use by Customer over the Internet. Micro Focus targets to provide Customer access to the SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9 % ("Solution Uptime").

Measurement Method
Solution Uptime 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, Solution Support Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) 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.

Boundaries and Exclusions

Solution Uptime 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
- Force majeure events
- 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 SaaS Upgrades

Online Support Availability SLO

Online Support Availability is defined as the SaaS support portal https://support.cyberreshelp.com, being available for access and use by Customer over the Internet. Micro Focus targets to provide Customer access to the SaaS support portal on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.9% ("Online Support Uptime").

Measurement Method

Online Support Uptime 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, Online Support Uptime will be measured using the measurable hours in the quarter (total time minus planned downtime, including maintenance, upgrades, etc.) 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.

Boundaries and Exclusions

Online Support Uptime shall not apply to or include any time during which the SaaS support portal 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
- Force majeure events
- Actions or inactions 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 SaaS Upgrades

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the support described herein. It is defined as the acknowledgment of the receipt of Customer's request and the assignment of a case number for tracking purposes. Initial SaaS Response will come as an email to the requester and include the case number and links to track it using Micro Focus online customer portal. The Initial SaaS Response Time covers both service request and support requests. Micro Focus targets to provide the Initial SaaS Response no more than one hour after the successful submission of Customer's request.

SaaS Support SLOs

There are two types of SaaS Support SLOs: Service Request and Support Request SLOs:

- The Service Request SLO applies to the majority of routine system requests. This includes functional system requests (product add/move/change), informational, and administrative requests.
- The Support Request SLO applies to issues that are not part of the standard operation of the service, and which causes, or may cause, an interruption to or a reduction in the quality of that service.

The Response and Resolution Targets are provided as guidelines and represent typical request processing by Micro Focus SaaS support teams. They in no way create a legal requirement or obligation for Micro Focus to respond in the stated time. The Response and Resolution Targets, including their scope and determining factors (such as impact and urgency), are further described above in the scheduled maintenance section.

Termination Data Retrieval Period SLO

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

Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to SaaS. Micro Focus' 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 SaaS • Manages contract issues
Project Manager	• Coordinates customer resources as necessary • Serves as the point of contact between the customer and Micro Focus • Drives communication from the customer side

	• Serves as the point of escalation for issue resolution and service-related issues
Administrator	• Serves as the first point of contact for SaaS end users for problem isolation • Performs SaaS administration • Provides Level 1 support and works with Micro Focus to provide Level 2 support • Coordinates end-user testing as required • Leads ongoing solution validation • Trains the end-user community • Coordinates infrastructure-related activities at the customer site • Owns any customization
Subject Matter Expert	• Leverages the product functionality designed by Customer's SaaS administrators • Provides periodic feedback to the SaaS Administrator

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Customer Service Centre (CSC)	• Primary point of contact for service requests. The customer can contact the Service Operations Center for all services such as support and maintenance, or issues regarding availability of SaaS • Provides 24x 5 application support with on call available for Severity 1 issues 24 x 7
Operations Staff (Ops)	• Monitors the Micro Focus systems and SaaS for availability • Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus's standard practices • Provides 24x7 SaaS infrastructure support

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 a destination endpoint capable of receiving Adversary Signals SaaS Insights via Syslog
- SaaS, including Adversary Signals Insights, will be delivered remotely in English only

- An Adversary Signals Order Term is valid for a single Adversary Signals tenant deployment, which cannot be changed during the Adversary Signals 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
- Customer will establish and follow secure practices for individual account-based access for accountability and traceability

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’ 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.