# Service Description

## OpenText Core Threat Detection and Response

**July 2025**

opentext™

## Contents

This Service Description describes the components and services included in OpenText Core Threat Detection and Response (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.opentext.com/about/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

OpenText Core Threat Detection and Response provides a cloud-based enterprise service that is intended to analyze telemetry from customer security systems and detect threats based on a combination of behavioral analytics and correlation of behavioral anomalies and indicators of compromise.

### SaaS Delivery Components

| SaaS Delivery Components | |
|---|---|
| **One production instance** | ✓ |
| **Insider Security services** | O |
| ✓ **= Included** | |
| **O = Optional for a fee** | |

The OpenText Core Threat Detection and Response 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.

Insider Security services are also available, optionally. Please consult the corresponding data sheets.

### SaaS Operational Services

| Operational Services | |
|---|---|
| **Help Desk Support** | ✓ |
| ✓ **= Included** | |

Core Threat Detection and Response leverages generative artificial intelligence (AI) with a third-party Large Language Model (LLM) to generate summaries of entity activity. Micro Focus does not guarantee the accuracy of AI-generated explanations. It is Customer's responsibility to apply judgment and consider multiple sources before making any decisions. *Customer acknowledges and agrees that Micro Focus shall have no liability or responsibility for any claims, causes of action, losses, harm, or any other liability resulting from Customer's use of such AI functionality.*

## Architecture Components

The Core Threat Detection and Response Offering is a SaaS-based analytics engine that consumes IT security event logs, analyzes those events for risky and unusual behaviors, as well as patterns of behavior, and provides daily results back. Logs are periodically sent to the analytic engine for analysis, and analytical results are published daily via the Core Threat Detection and Response UI for exploration. The offering is multi-tenant, meaning that each customer receives their own unique tenant. This tenant segregates and secures Customer's analytics results and underlying data from all other tenants.

## Application Administration

Customer will access Core Threat Detection and Response using a web browser and the URLs provided to it. Once securely logged in, Customer can perform administrative tasks such as configuring access to data, configuring user access, as well as exploring analytics results.

## Service Support

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

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 maintain a list of authorized users who may contact Micro Focus for support. Customer's authorized users may contact Micro Focus for support via the Web portal 24 hours a day, 7 days a week.

## 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 available to Customer online at: https://support.cyberreshelp.com

## Capacity and Performance Management

The Core Threat Detection and Response environment is continually monitored for performance status. Proactive capacity and performance management procedures are in place to ensure the architecture of the environment meets Customer needs. The architecture allows for additional capacity for 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 tested and reviewed prior to implementation to ensure they are appropriately scheduled and tested before promotion to production.

### Preview Features

SaaS may include capabilities that are incomplete or not fully tested at the time of release ("Preview Features"). These capabilities are "feature complete" but may not be fully tested and are included for evaluation purposes, not for any development, production, distribution or commercial purpose. The Preview Features are provided "as is" and there are no warranties or obligations, including the obligation for Micro Focus to provide support. Customer agrees to promptly report to Micro Focus all problems (including errors, failures, nonconforming results, and unexpected performances) and any comments regarding the Preview Features. Micro Focus may choose not to release a final version of the Preview Features or even if released, to alter features, specifications, capabilities, functions or other characteristics of the Preview Features.

Preview Features will be labelled as "Preview" in the Core Threat Detection and Response user interface.

## 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 availability to SaaS and SaaS Data for Customer following an outage or similar loss of service for SaaS.

### SaaS Data

Customer is solely responsible for the data, text, audio, video, images, software, and other content input into a Micro Focus system or environment during Customer's (and its Affiliates' and/or Third Parties') access or use of Micro Focus SaaS ("SaaS Data"). The following types of SaaS Data reside in the SaaS environment:

**Data Type** - A category of log data emitted by a set of technologies that have a common goal. These category types are usually part of a common market.

**Data Source** - A technology that emits log data that fits into a particular data type. Typically, the name of a vendor or product name that is categorized within that market.

Example: Microsoft Entra ID and Microsoft Defender for Endpoint are Data Sources.

Supported data types include:

- Access
- Authentication
- Email
- Endpoint
- Source Code Repository
- Remote Access (e.g. VPN)
- Network (e.g. Web Proxy)

Micro Focus performs a backup of SaaS Data every two (2) hours. Micro Focus retains each backup for the most recent seven (7) days.

Micro Focus' standard storage and backup measures are Micro Focus' only responsibility regarding the retention of the SaaS Data, despite any assistance or efforts provided by Micro Focus to recover or restore the SaaS Data. Customer may request via a service request for Micro Focus to attempt to restore SaaS 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.

In addition to the event data corresponding the data sources collected, analytical results including alerts, analyst annotations, and risk scores will be included in the backups.

### 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**
Micro Focus SaaS utilizes cloud-native functions such as replication between primary and secondary availability zones to ensure data availability and recoverability. Replication is used between primary and standby zones to facilitate an RPO of 2 hours. 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
- 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 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

## 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' 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. A summary report or similar documentation will be provided to Customer upon request. 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.

Customer initiated security testing is not permitted, which includes application penetration testing, vulnerability scanning, application code testing or any other attempt to breach the security or authentication measures of the SaaS.

## 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 Employees and Subcontractors

Micro Focus requires 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 SaaS Data. 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.

## Data Subject Requests

Micro Focus will refer to Customer any queries from data subjects in connection with SaaS Data.

## Scheduled Maintenance

To enable Customer to plan for scheduled maintenance by Micro Focus, Micro Focus reserves predefined timeframes to be used on an as-needed basis. Micro Focus reserves a weekly two (2) hours window (Sunday 00:00 to 02:00 Pacific Standard Time) and one (1) monthly four (4) hour window (Sunday in the 00:00 to 08:00 Pacific Standard Time block). These windows will be used on an as-needed basis.

Planned windows will be scheduled at least two (2) weeks in advance when Customer action is required, or at least four (4) days in advance otherwise.

### 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 SaaS Order Term unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

Micro Focus determines whether and when to apply a SaaS Upgrade to Customer's SaaS. 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 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' 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.

## 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.

1. **SaaS Provisioning Time SLO**
   SaaS Provisioning Time is defined as SaaS being available for access over the internet. Micro Focus targets to make SaaS available within five (5) business days of either (1) Customer's Order for SaaS being booked within the Micro Focus order management system or (2) Micro Focus' receipt of Orders placed directly through Azure Marketplace.

   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-premise components are not in scope of the SaaS Provisioning Time SLO.

   Additionally, the import of SaaS Data into the application is not in scope of the SaaS Provisioning Time SLO.

2. **SaaS Availability SLO**
   SaaS Availability is defined as 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 99.9 % ("SaaS Uptime").

3. **Measurement Method**
   SaaS 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, SaaS 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**
   SaaS 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

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").

1. **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.

2. **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.

## 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 SaaS Order Term.

# Standard Service Requirements

## 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<br>• Owns the business relationship with the range of departments and organizations using SaaS<br>• Manages contract issues |
| **Administrator** | • Serves as the first point of contact for SaaS end users for problem isolation<br>• Performs SaaS administration<br>• Provides tier-1 support and works with Micro Focus to provide tier-2 support<br>• Coordinates end-user testing as required<br>• Leads ongoing SaaS validation<br>• Trains the end-user community<br>• Coordinates infrastructure-related activities at the customer site<br>• Owns any customization |
| **Subject Matter Expert** | • Leverages the product functionality designed by Customer's SaaS administrators.<br>• 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<br>• Provides 24x7 application support |
| **Operations Staff (Ops)** | • Monitors the Micro Focus systems and SaaS for availability<br>• Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus' standard practices<br>• 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
- 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 either (1) the date on which Customer´s Order is booked within the Micro Focus order management system or (2) Micro Focus' receipt of Orders placed directly through Azure Marketplace
- The import of SaaS 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
- Customer utilizes Microsoft EntraID and Microsoft Defender for Endpoint

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.