Service Description

OpenText™ Core Application Security Standard Service (Fortify on Demand)

May 2025

Contents

This Service Description describes the components and services included in OpenText™ Core Application Security (Fortify on Demand) (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 Application Security (SaaS) is a remotely delivered, cloud-based application security-as-a-service. Application security testing is performed and reviewed by security experts using application testing technologies and manual techniques. All customers are provided access to our technical account support team. Customer can choose the SaaS data center where their data will be stored, subject to availability and support as determined by Micro Focus. All SaaS Data remains in the chosen data center or its back-up facility located in the same AWS Region.

OpenText™ Core Application Security provides static application security testing (SAST), dynamic application security testing (DAST), mobile application security testing (MAST) and software composition analysis (SCA). The customer may access reports which detail the findings of the assessment(s) in a standard format by accessing the SaaS web application portal and/or application programming interface (API). SaaS also offers add-ons and supplemental support services.

SaaS Delivery Components

SaaS Delivery Components

One OpenText™ Core Application Security production tenant hosted in Customer's selected OpenText™ Core Application Security Data Center with Standard Support	✓

✓ **= Included**

O = Optional for a fee

SaaS Operational Services

OpenText™ Core Application Security (SaaS) Operational Services includes a range of options for assessments and support for purchase, all of which are described below and subject to the legal quotation.

Applications and Developers are defined under Application Administration (below). A Subscription is the twelve (12) month period in which one Application can be assessed repeatedly. For a multi-year purchase, a new Subscription starts on the anniversary of the SaaS Order Term. One Application cannot be exchanged for a different Application during a Subscription. Only one (1) assessment may be performed at a time per Application.

SAST, DAST, and MAST are made available by purchasing and redeeming SaaS Assessment Units (AUs). AUs are pre-paid credits that are redeemed for a single assessment or Application Subscription and are valid for twelve (12) months during the SaaS Order Term or, if less than twelve (12) months remain in the SaaS Order Term, then until the termination of the SaaS Order Term. A customer may purchase one or more years of AUs

on a single Order. For a multi-year purchase, the purchased quantity of AUs is issued on the anniversary of the SaaS Order Term. Each year's allotment of AUs must be used within twelve (12) months and are not "rolled over" to subsequent years.

A single assessment includes one (1) remediation validation assessment which must be submitted within thirty (30) days of the assessment.

Static Application Security Testing
Micro Focus will perform a static assessment using OpenText™ Static Application Security Testing (SAST) of the Application code uploaded by the Customer.

Assessment Type	Static Assessment	Static+ Assessment
OpenText SAST	◆	◆
Microservice Applications	◆	N/A
Security Expert Review	One Assessment (Subscription Only)	◆
Single Assessment	1 Assessment Unit	2 Assessment Units
Application Subscription	4 Assessment Units	6 Assessment Units
SAST Aviator Add-on Subscription (per Application)	1 Assessment Unit	1 Assessment Unit

Additional Notes:

- New assessments can be queued if requested when an assessment is already running.
- Security Expert Review includes false positive removal.
- Static Assessment Application Subscriptions include a Security Expert Review for one (1) assessment (typically the initial assessment). Static Assessment single assessments do not include a Security Expert Review.

SAST Aviator audits, explains, and if applicable, suggests code fixes for security issues identified by a SaaS Static or Static+ Assessment. A SAST Aviator Subscription is an optional add-on to a SaaS Static or Static+ Assessment that can be purchased for an additional 1 Assessment Unit (AU) per Application.

SAST Aviator leverages generative artificial intelligence (AI) with a third-party Large Language Model (LLM) to generate the content described above. Access to and use of SAST Aviator is subject to Customer agreeing to additional LLM terms (including the Acceptable Use Policy and rights to use) that are available when Customer configures use of SAST Aviator. Micro Focus does not guarantee the accuracy of AI-generated responses. 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.*

Static Assessment Developer Subscriptions may be utilized at a rate of sixteen (16) Assessment Units for ten (10) Developers. SAST Aviator Add-on Subscriptions may be utilized at a rate of four (4) Assessment Units for ten (10) Developers. Static Assessment Developer Subscriptions may not be combined with Application Subscriptions. Static+ Assessments are not available as Developer Subscriptions.

Dynamic Application Security Testing
Micro Focus will perform an automated, authenticated OpenText™ Dynamic Application Security Testing

(DAST) of a web or API application.

Assessment Type	DAST Automated Assessment	Dynamic Assessment	Dynamic+ Assessment
OpenText DAST	◆	◆	◆
Web Applications	◆	◆	◆
API Applications	◆	◆	◆
Login Macro Creation	Customer Provided	◆	◆
Security Expert Review	N/A	◆	◆
Manual Testing	N/A	N/A	◆
Single Assessment	1 Assessment Unit	2 Assessment Units	6 Assessment Units
Application Subscription	2 Assessment Units	6 Assessment Units	18 Assessment Units
DAST Automated Add-on Service	1 Assessment Unit	N/A	N/A

Additional Notes:

- Security Expert Review includes false positive removal.
- Manual testing includes up to eight (8) hours of analysis per assessment by a SaaS expert using the SaaS testing methodology.

For each Application, DAST Automated Add-on Service includes (1) assistance creating a one-time login macro; and (2) a review of prioritized results by a Micro Focus security expert from the initial scan.

New findings from subsequent scans will not be reviewed by a Micro Focus security expert. One DAST Automated Add-on Service may be purchased per Application.

Mobile Application Security Testing

Micro Focus will perform Mobile Application Security Testing of the mobile application client iOS or Android binary uploaded by the Customer and for Mobile+ Assessment, backend APIs owned by the Customer which are utilized by the mobile application.

Assessment Type	Mobile Assessment	Mobile+ Assessment
Mobile Binary Analysis	◆	◆
Endpoint Reputation Analysis	◆	◆
Security Expert Review	◆	◆
OpenText DAST of APIs	N/A	◆
Manual Testing	N/A	◆
Single Assessment	1 Assessment Unit	6 Assessment Units
Application Subscription	4 Assessment Units	18 Assessment Units

Additional notes:

- Endpoint Reputation Analysis is performed on URL endpoints discovered during binary analysis.
- Security Expert Review includes false positive removal.
- OpenText DAST of APIs includes an automated, authenticated DAST assessment of Customer-owned API endpoints invoked by the mobile application client as identified by Micro Focus.
- Manual Testing includes up to eight (8) hours of analysis per assessment across the mobile application binary, network and backend APIs by a SaaS expert using the SaaS testing methodology.

Software Composition Analysis

Software Composition Analysis Assessments allow the customer to perform automated software composition analysis to identify open-source components and other third-party software that is present in application code. The results of a Software Composition Analysis Assessment include security issues and license information associated with the identified components. Software Composition is available for purchase as an Application Subscription or a Developer Subscription.

OpenText™ Core SAST Aviator (SAST Aviator)

OpenText™ Core SAST Aviator (SAST Aviator) provides a cloud-based, multi-tenant enterprise service for auditing and remediating findings produced by OpenText SAST off cloud or private cloud solutions. SAST Aviator is accessed via command line software to send SAST scan results from Customer's Software Security Center instance to SAST Aviator for processing. SAST Aviator assesses whether findings produced by the SAST scan are correct (true positive) or not (false positive) and provides a comment explaining the assessment. In the case of true positives, SAST Aviator will advise how to remediate the issue. The SAST Aviator output will be stored as audit information in Software Security Center.

Vulnerability and audit information is not stored within the SAST Aviator service. The service only retains statistical data related to the delivery and usage of the service, such as number of issues processed, performance data and other operational metrics. Individual issues are only assessed once. SAST Aviator may implement processing limits on the number of issues assessed on a single assessment.

SAST Aviator leverages generative artificial intelligence (AI) with a third-party Large Language Model (LLM) to generate the content described above. Access to and use of Fortify Aviator is subject to Customer agreeing to additional LLM terms (including the Acceptable Use Policy and rights to use) that are available when Customer configures use of Fortify Aviator. Micro Focus does not guarantee the accuracy of AI-generated responses. 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.*

SAST Aviator is available for purchase as an Application Subscription or a Developer Subscription. When purchased as Developer Subscriptions, the maximum number of allowed Applications will be forty (40) percent of the quantity of Developer Subscriptions purchased. For example, if twenty-five (25) Developers Subscriptions are purchased, up to ten (10) Applications may be assessed with SAST Aviator during the Subscription.

Architecture Components

OpenText™ Core Application Security is a cloud-based Application security platform portal that is used for scheduling application security assessments and consuming the results of those assessment results via dashboards and reports. SaaS is a multi-tenant environment, meaning that each customer receives their own unique tenant. This tenant segregates their application testing data from all other tenants. No components or software are required for installation on the customer premise to facilitate application testing or result consumption included in the SaaS (excluding SAST Aviator, which may be used with Customer's existing on-premise licenses).

Application Administration

Applications and Developers are defined according to the Assessment Types and Services below.

Static Application Security Testing
For static assessments, an Application is defined as a deployable unit of code consisting of a collection of source and/or byte code instruction files that:

- Meets the OpenText™ Static Application Security Testing (SAST) minimum requirements for currently supported languages, which should be successfully compiled prior to submission of the application
- Can deliver some or all the functionality of a business application
- Can be assessed with a single translation or scan by OpenText SAST
- Does not include any loosely coupled components
- Can be configured to run on an application server, if applicable (e.g., a Web Application Archive [WAR] or Enterprise Archive [EAR] file for a Java application or a solution file for a .NET application)

A microservice is a small, modular service that runs as an independent, loosely coupled process and communicates through a well-defined, lightweight mechanism to serve a single function of a business application. For Applications built using a microservices architecture, a Static Subscription entitles the customer to test up to ten (10) microservices that form some or all the Application. For all other static application security assessment services, each microservice is considered a separate Application. Each microservice must be submitted independently in a single ZIP file of one hundred (100) megabytes or less in size. Microservice Applications do not include a review by a SaaS security expert on the initial assessment.

A Developer is defined as any individual that has: (1) committed code to the applications to be assessed during the 90 days prior to assessment; or (2) the most recent individual who has made changes to the application code if no code commits have been made in the past 90 days. Only code committed by licensed Developers may be assessed. For the avoidance of doubt, at least one (1) Developer is required for each application assessed under the Developer model. Customer is required to submit a quarterly report of licensed Developers to Micro Focus.

Dynamic Application Security Testing
For all dynamic assessments, an Application is defined as a fully qualified domain name (FQDN). For example, for www.example.com

- www.example.com is the FQDN and is the Application to be assessed.
- www.example.com/news/ is the same hostname and FQDN and so is the same Application.
- community.example.com is a different subdomain and FQDN and so is a different Application.
- www.example.co.uk is a different domain name and FQDN and so is a different Application.
- Non-production environments (like staging or development) hosting the same Application can be grouped and submitted as one (1) Application under different releases.

The Application can only have a single authentication management system with the following exceptions:

- Forms authentication and one (1) network authentication (basic/digest/NTLM) is allowed.
- Forms authentication, one (1) network authentication and application generated authentication such as bearer tokens is allowed. User logins may not be “daisy chained”. For example, two (2) Forms authentication mechanisms are not permitted.

Customer will provide port 80/443 access to all Applications that are to be assessed for remote testers. If they are internal Applications, access will be provided for the SaaS testing team using IP application and user credentials are functioning prior to the security assessment. In addition, all functional and performance testing should be completed by this time, and the Application’s code should be frozen for the duration of the security test engagement.

For Applications that utilize anti-automation technology, such as Multi-Factor Authentication (MFA) or CAPTCHA, Micro Focus recommends the Customer disable the anti-automation technology. If Customer chooses or is not able to disable the anti-automation technology, coverage of the OpenText™ Dynamic Application Security Testing (DAST) assessment may be reduced, such as by performing an unauthenticated assessment or not assessing functionality blocked by CAPTCHA. On a Dynamic+ Assessment, manual testing supports email one-time-password (OTP) when assessing applications with MFA.

SaaS IP addresses must be whitelisted through all Customer network devices, such as web application firewalls (WAFs), network firewalls and intrusion prevention systems (IPSs). Testing requires unfettered access to the application (URLs, APIs) to receive the benefit of this service. Failure to do so will produce poor results including false negatives. The scope of this service does not include any testing or bypassing of mitigating controls in place (WAFs/Firewalls/IPS/Captcha).

For API Applications, a maximum of fifty (50) API endpoints will be assessed. Customer must provide one (1) definition of the API endpoints as follows:

- Dynamic Assessments
  - REST API- OpenAPI JSON specification or Postman collection with valid values for all parameters and a hard coded and long-lived authentication token
  - GraphQL- Postman collection with valid values for all parameters and a hard coded and long-lived authentication token
- Dynamic+ Assessments
  - REST API- OpenAPI JSON specification or Postman collection
  - GraphQL- Postman collection with valid values for all parameters
  - SOAP – single SOAP WSDL file working examples, with valid values for all parameters, must be provided

For Dynamic+ website assessments, in addition to assessing the Application as defined above, the assessment will also test for vulnerabilities on any linked endpoints called by the Application, such as authentication or backend APIs, that are located on Customer-owned domains specified by the Customer. Endpoints on third-party subdomains will not be assessed.

Mobile Assessments
For mobile assessments, an Application is defined as a single installable mobile binary for a single hardware platform. Mobile applications submitted for testing must be in the form of a compiled IPA (iOS), AAB (Android) or APK (Android).

Software Composition Analysis
Software composition analysis assessments can be conducted separately or in conjunction with a static assessment. The Application and Developer definitions for static assessments, including reporting requirements, applies to all software composition analysis assessments.

For Applications built using a microservices architecture, up to ten (10) microservices may be treated as a single Application. Each microservice must be submitted independently in a single ZIP file of one hundred (100) megabytes or less in size.

SAST Aviator
For SAST Aviator, an Application is defined as a unique code base analyzed by OpenText Static Application Security Testing (Fortify Static Code Analyzer) to produce a single FPR file.

A Developer is defined as any individual that has: (1) committed code to the applications to be assessed during the 90 days prior to assessment; or (2) the most recent individual who has made changes to the application code if no code commits have been made in the past 90 days. Only code committed by licensed Developers may be assessed. For the avoidance of doubt, at least one (1) Developer is required for each application

assessed under the Developer model. Customer is required to submit a quarterly report of licensed Developers to Micro Focus.

Service Support

Micro Focus staffs and maintains a 24x7x365 Service Operations Center, which will be the single point of contact for all issues related to SaaS support. 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.

Online support and product documentation are available within the SaaS web portal.

Support Services	Standard Support	Managed Support	Enhanced Support	Premium Support
Welcome Pack	◆	◆	◆	◆
Self Service Portal	◆	◆	◆	◆
Help Desk Support	◆	◆	◆	◆
Customer Success Manager		◆	◆	◆
Onboard Customer Development Teams		1 team	4 teams	20 teams
Results Review Calls		1 per SaaS Order Term	2 per month	8 per month
Integration Support Sessions			1	4
Application Onboarding Assistance			◆	◆
AppSec Program Support				◆

Standard Support is included with all purchases. Managed Support, Enhanced Support and Premium Support are available for optional purchase. Managed Support is included for all purchases of one hundred (100) Assessment Units or more.

Onboard Customer Development teams
Micro Focus will provide a one (1) hour session for each Customer development team, which includes a live SaaS portal walk through, overview of integration tools and API, and guidance for integrating SaaS into Customer's development toolchain using available integrations and tools.

Integration Support Service
Micro Focus will provide the following services associated with one (1) custom integration:

- One (1) hour call to discuss high-level design of specific integration requirement
- Identify existing sample code (if available)
- Identify SaaS API calls relevant to implementation of custom integration
- Provide guidance to Customer in use of SaaS API for Customer to develop the integration

Results Review Call
Micro Focus will provide a one (1) hour call with Customer to review assessment results for one (1) application including:

- Explain findings produced by OpenText Core Application Security SAST, DAST, MAST or SCA

- Provide guidance on advanced remediation features of the SaaS product
- Provide advice and guidance for applying organizational policies or specific application coding patterns to enable Customer to configure SaaS and/or remediate findings

Additional packages of four (4) results review calls per month are available for optional purchase.

Application Onboarding Assistance
Micro Focus will create up to two thousand (2,000) applications, with one release or microservice per application using the default configuration, in Customer's SaaS tenant. Customer must provide a CSV file of applications to be created in the format specified by OpenText within 30 days of tenant creation. A single user will be designated as the owner of the applications created during this process.

AppSec Program Support
Micro Focus will provide the following services:

- Advise on program kickoff, milestone and AppSec goal planning
- Share current Application Security best practices
- Assist Customer Application Security team with leveraging SaaS in their organization
- Assists Customer's technical writer in preparing customized SaaS training

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 at https://status.fortify.com/.

Capacity and Performance Management

The 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.

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

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

- Application Meta Data
- Application Source Code
- Application Binaries

SaaS uses SaaS Data to produce Application vulnerability information. In addition, SaaS stores business contact information for the users of the service. These are typically Customer employees in security and development.

Permitted Uses

Micro Focus will use SaaS Data only as necessary to provide the SaaS, provide or maintain the security and integrity of the SaaS, provide technical support to the Customer, improve the performance and accuracy of the SaaS or as otherwise required by law (the "Permitted Uses").

Micro Focus owns all rights to any data generated by Micro Focus during the delivery of SaaS ("Metadata"). Metadata further includes, without limitation, data generated through the Fortify Audit Assistant platform. Metadata will be anonymized and will not contain Customer Personal Information. To the extent required by law, Customer grants Micro Focus a perpetual, royalty free license to all Metadata for any lawful purposes.

Data Retention

Application, user and assessment results and user data retention are managed by the Customer and can be deleted using features of the SaaS service. Application event logs, which include access attempts, are retained for up to thirteen (13) months. Application code uploaded by Customer is retained for up to fifteen (15) days. Data is securely deleted from the backup media in accordance with the Backup Retention Time after data is deleted from the SaaS service.

Micro Focus performs a backup of SaaS Data every day. Micro Focus retains each backup for the most recent fourteen (14) days.

Micro Focus' standard storage and backup measures are Micro Focus' 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 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 performs both on-site and off-site backups with a 24-hour recovery point objective (RPO). Backup cycle occurs daily where a local copy of production data is replicated on-site between two physically separated storage instances. The backup includes a snapshot of production data along with an export file of the production database. The production data is then backed up to a different site. Micro Focus uses storage and database replication for its remote site backup process. The integrity of backups is validated by (1) real time monitoring of the storage snapshot process for system errors, and (2) and annual restoration of production data from an alternate site to validate both data and restore flows integrity.

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

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 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) hour window (Wednesday 00:00 to 02:00 in the local time zone of the SaaS datacenter) and one (1) monthly twenty-four (24) hour window (between Friday & Sunday SaaS datacenter). 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.

SaaS Datacenter	Local Time Zone
AMS	US Eastern Time Zone
EMEA	Greenwich Mean Time Zone
APAC	Australian Eastern Time Zone
SINGAPORE	Singapore Time Zone

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 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.

SaaS Provisioning Time SLO

SaaS 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 Order for SaaS being booked within the Micro Focus order management system.

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 of the SaaS 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.

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 99.5 % ("SaaS Uptime").

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 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
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

Security Assessment Time SLO

Security Assessment Time is defined as the length of time from the date the application assessment was requested to be started and the date the results are made available through the SaaS. If an assessment is queued the Security Assessment Time is measured from when the assessment actually starts. The Security Assessment Time excludes weekends and any time the assessment is paused while awaiting feedback from Customer regarding questions from a SaaS security experts about the application. Micro Focus targets to deliver 95% of assessments within the Security Assessment Time for each assessment type.

Assessment Type	Automated Audit	Security Expert Review
Static Assessment	Four (4) hours[1]	Two (2) days

Static+ Assessment	Four (4) hours[1]	Two (2) days
DAST Automated	Twelve (12) hours[3]	N/A
Dynamic Website Assessment	N/A	Two (2) days
Dynamic+ Website Assessment	N/A	Three (3) days
Dynamic API Assessment	N/A	Two (2) days
Dynamic+ API Assessment	N/A	Three (3) days
Mobile Assessment	Ten (10) minutes[2]	One (1) day
Mobile+ Assessment	N/A	Four (4) days

1 Typical turnaround is less than fifteen (15) minutes for most customers subject to conditions below

2 Audit preference is "Automatically publish (no audit)"

3 For DAST Automated SLOs are only applicable to API postman and workflow driven scans SLO does not apply for timeboxed scans.

Static Security Assessment Time shall not apply to any of the following exceptions

- Application has not been packaged correctly as per SaaS best practice guidelines, which are found (in SaaS product documentation)
- The application payload exceeds 1,000MB

Dynamic and Mobile Security Assessment Time shall not apply to any of the following exceptions:

- Customer does not provide SaaS continuous 24-hour per day access and fully operational test credentials to assess the application that is in scope
- SaaS is not able to configure security testing tools to use a minimum of fifteen (15) concurrent connections continuously to assess a single application with an average response time of less than 600ms to an HTTP/HTTPS request
- Mobile binary is obfuscated or is not prepared as per SaaS best practice guidelines

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.

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 • 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 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 tier-1 support and works with Micro Focus to provide tier-2 support • Coordinates end-user testing as required • Leads ongoing SaaS 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 24x5 application support with limited resource supporting over the weekend
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 standard practices • Provides 24x5 SaaS infrastructure support
Customer Success Manager (CSM)	• Named, shared resource that serves as a single point of contact for Customer • Schedules regular check in calls to review adoption and use of SaaS

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 OpenText™ Core Application Security tenant, 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 SaaS Data into SaaS during the implementation requires that the information is made available to Micro Focus at the appropriate step of the SaaS 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

Customer acknowledges that some of the services are designed to test the security of computer software, and the software and/or testing services used may reveal or create problems in the operation of the systems tested. The testing may result in disruptions of and/or damage to the customer's or the customer's third-party service provider's information systems and the information and data contained therein, including but not limited to denial of access to a legitimate system user, automatic shutdown of information systems caused by intrusion detection software or hardware, or failure of the information system. Micro Focus endeavors to help minimize disruptions to the application or network while performing any automated scanning, manual validation, or penetration testing. Customer accepts the risk of such possibility and hereby waives all rights, remedies, and causes of action against Micro Focus and releases Micro Focus from all liabilities arising from such problems.

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.