Service Description

Fortify Hosted

Jaunuary 2024

MICRO FOCUS
is now opentext™

Contents

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

Standard Service Features

High Level Summary

Micro Focus Fortify Hosted provides a cloud-based enterprise service for automating application security programs. It enables management, development, and security teams to work together to triage, track, validate and manage software security activities.

Fortify Hosted enables Static Application Security Testing (SAST), Dynamic Application Security testing (DAST) and optionally Software Composition Analysis (SCA) to be fully integrated into the Customer's Software Development Lifecycle.

Micro Focus is responsible for the provision of Fortify Hosted on an AWS cloud platform and delivers ongoing infrastructure, application, and support service remotely.

SaaS Delivery Components

SaaS Delivery Components	
One Fortify Hosted Base Package hosted on Customer's preferred AWS Region Availability Zone	✓
Sonatype Lifecycle Hosting	O
Additional SAST or DAST Scan Machine	O
Option to upgrade a standard configuration SAST or DAST Scan Machine to the upgraded configuration	O
Option to upgrade the Standard configuration Sandbox Environment to the Upgraded configuration Sandbox Environment. Additional Standard or Upgraded Scan Machines can also be purchased for this environment	O
Additional user licenses for the Fortify End-User Tools available on a per named user basis or an unlimited enterprise license	O
✓ **= Included**	
O **= Optional for a fee**	

SaaS Operational Services

SaaS Operational Services	
Customer Success Manager	✓

SAST Advanced Support	O
DAST Advanced Support	O

✓ = Included

O = Optional for a fee

Architecture Components

Micro Focus Hosted consists of a single tenant cloud-based solution with a web-based user interface allowing the Customer to configure, perform and manage application security assessments. In addition, the functionality can be accessed via a suite of tools and a comprehensive API enabling application security assessments to be integrated into the Customer's Software Development Lifecycle. All connectivity between Fortify Hosted and the Customer's environment is via the internet from a restricted range of IP addresses provided by the Customer or Site-to-Site VPN.

It consists of the following components

- Software Security Center
  Software Security Center (SSC) is Micro Focus SSC hosted on the SaaS platform. It is the central management system that allows a Customer to manage their enterprise application security program. Up to 1TB of database storage is included.

- License and Infrastructure Management
  License and infrastructure Management (LIM) is Microfocus LIM hosted on the SaaS platform. It allows central management of the license for the SAST and DAST components of Fortify Hosted.

- Audit Assistant
  Audit Assistant is a feature of SSC that uses machine learning to improve the quality of SAST findings. If Customer choses to use this feature, it will require a connection to the multi-tenant cloud based Fortify Scan Analytics server

- ScanCentral SAST Controller
  ScanCentral SAST Controller is Micro Focus ScanCentral SAST Controller hosted on the SaaS platform. It is an extension to SSC that controls the queuing and execution of SAST assessments.

- ScanCentral SAST Scan Machine
  ScanCentral SAST Scan Machine is Micro Focus ScanCentral SAST sensor hosted on the SaaS platform. It performs the SAST assessment by executing the Micro Focus Fortify Static Code Analyzer. The following configurations are available:
  - Standard - 8 vCPUs, 32 GB RAM on Linux
  - Standard - 4 vCPUs, 32 GB RAM on Windows
  - Upgraded - 16 vCPUs, 64 GB RAM on Linux
  - Upgraded - 8 vCPUs, 64 GB RAM on Windows

- ScanCentral DAST Controller
  ScanCentral DAST Controller is Micro Focus ScanCentral DAST Controller hosted on the SaaS platform. It is an extension to SSC that controls the queuing and execution of DAST assessments. Up to 1TB of database storage is included.

- ScanCentral DAST Scan Machine
  ScanCentral DAST Scan Machine is Micro Focus ScanCentral DAST sensor hosted on the SaaS platform. It performs the DAST assessment by executing Micro Focus Fortify WebInspect. The following configurations are available:
  - Standard - 4 vCPUs, 32 GB RAM on Linux
  - Upgraded - 8 vCPUs, 64 GB RAM on Linux

- Sonatype Lifecycle Hosting
  Sonatype Lifecyle Hosting is the hosting of Sonatype IQ Server on the SaaS platform. Sonatype IQ Server performs Software Composition Analysis (SCA) assessments and monitoring. Up to 1TB of database storage is included.

- Fortify End-User tools
  Fortify End-User tools are a range of end-user tools that can be used by the Customer to submit assessment requests and work with the results. These include:
  - Fortify Software Security Center Web Interface
  - Fortify Audit Workbench
  - Fortify Security Assistant
  - IDE plugins
  - Build tools
  - CI/CD plugins
  - Fortify DAST tools

- Sandbox Environment
  A Micro Focus hosted, single-tenant test environment that includes the major Fortify Hosted components and 2 Scan Machines. This environment is for the Customer to perform integration and upgrade testing. The following configurations are available:
  - Standard - Reduced CPU, RAM, and database size
  - Upgraded – Same specification as production environment

Fortify Hosted is acquired by purchasing a Fortify Hosted Base Package consisting of:

- Software Security Center
- License and Infrastructure Management
- ScanCentral SAST Controller
- ScanCentral DAST Controller
- A total of 3 standard configurations of ScanCentral SAST or DAST Scan Machines. The mix between SAST an DAST is chosen by the Customer
- Standard configuration Sandbox Environment

- License for 10 named users of the Fortify End-User Tools

At the time of purchase the Customer can request their preferred commercial AWS Region and Availability Zone for their instance of the Fortify Hosted solution, subject to availability and support for Fortify Hosted components as determined by Micro Focus.

In addition, the Customer can purchase the following options:

- Sonatype Lifecycle Hosting. This also requires the Customer to purchase
  - Sonatype Lifecycle User subscription
- Additional standard configuration SAST or DAST Scan Machines
- Option to upgrade a standard configuration SAST or DAST Scan Machine to the upgraded configuration
- Option to upgrade the Standard configuration Sandbox Environment to the Upgraded configuration Sandbox Environment. Additional Standard or Upgraded Scan Machines can also be purchased for this environment
- Additional user licenses for the Fortify End-User Tools available on a per named user basis or an unlimited enterprise license

Application Administration

The Customer will manage Fortify Hosted via the web user interface to Software Security Center where they can perform administrative tasks such as:

- User account management
- Managing applications and versions
- ScanCentral operations
- Configuring performance indicators and alerts
- Working with assessment results
- Generating reports

If any administrative task requires access to the underlying infrastructure the Customer can raise a support request and the task, if approved, will be performed by Micro Focus Operations staff.

Once per quarter, the Customer has the option of changing their selection of ScanCentral SAST and DAST Scan Machines. The change will be made at the next available scheduled maintenance window.

Service Support

Help-Desk support is included with all purchases. The Customer may contact Micro Focus through

- Email: CyberResSupport@microfocus.com
- CyberRes Portal: https://support.cyberreshelp.com
- Phone: Phone: +1 (855) 982-2261

The Micro Focus Support Team will either provide support to the Customer directly or coordinate delivery of this support. The severity of the request determines the response from the team.

Severity Level	Business Support	Severity Level Description
1	1 hour	Production system is down. The product is inoperable, resulting in a total disruption of work. No workaround is available.
2	3 hours	Major functionality failure. Operations are severely restricted, although work can continue in a limited fashion. A workaround is available.
3	6 hours	Minor functionality failure. Product does not operate as designed, resulting in a minor loss of usage. A workaround may be available.
4	1 business day	There is no loss of service. For example, this may be a request for documentation, general information, or a Software enhancement request.

The product documentation is available at:
https://www.microfocus.com/en-us/support/documentation

Training can be purchased at:
https://marketplace.microfocus.com/education

Customer Success Manager

Support from a Customer Success Manger is included with all purchases. The Customer is assigned a Customer Success Manager (CSM) as a primary point of contact to:

- Manage the on-boarding of the Customer to the Service
    - Validate connectivity from the Customer environment
        - Site-to-Site VPN configuration, if required
        - SSO configuration, if required
        - Test access from Web Browser and IDE
        - Test access from Customer's build environment
    - Live Service hand-over – Four (4) hour session
        - Review configuration
        - Walk-thru of SSC console
        - Submit sample static and dynamic scan
        - Review Logs
        - Review Results
        - Explain support process

*Note that the service requires Customer Personnel who are trained or experienced in using Fortify SSC with Scan Central. Training can be purchased separately.

- Periodic check-in calls
    - Eight (8) check-in calls can be made during the first eight (8) weeks of on-boarding (limit one per week). Check-in calls after the on-boarding period can be held once per month
    - These calls are with the Customer focal team and the CSM
    - These calls will include review of scanning activity, tickets raised and provide best practice guidance
- Manage service requests, such as support and maintenance services or issues regarding availability of the Fortify Hosted infrastructure

- Manage use of any optional services
- All support provided remotely by named CSM. CSM is a shared resource.

Enhanced Support
Enhanced Support is available for optional purchase. The Customer is assigned additional support resource(s) to proactively work with the Customer. The resource(s) will combine deep technical expertise in Fortify with a working knowledge of the Customer environment to

- Assist with problem identification and resolution to get issues resolved quickly and efficiently
- Submit enhancement and defect reports
- Provide technical advice and guidance
- Mentor the Customer's team to increase their knowledge
- Coordinate with Customer Success Manager (CSM) for escalation, coordination, and incident reviews

All support provided remotely. Total Enhanced Support effort is capped at 50 man-days per 12 months.

SAST Advanced Support

SAST Advanced Support is available for optional purchase. It is purchased in blocks of 25 person-days effort to be delivered over a 12-month period. SAST Advanced Support is requested through the CSM. 1 weeks' notice is required, and the minimum period is 4 hours.

SAST Advanced Support can be used to assist the Customer in the following areas:

- Packaging applications for scanning and optimizing settings
- On-boarding development teams
    - Demonstration of the relevant service features
    - Guidance for integrating Fortify Hosted into the Customer's development toolchain including build server and IDE's
- Integration Support
    - Workshop to agree high-level design of specific integration requirement
    - Identify existing sample code (if any) and provide to the Customer
    - Identify API calls required
    - Provide coaching to the client development teams in use of Fortify Hosted API to develop integration
- Auditing of scan results
- Results review calls
    - Explain why an issue is being flagged as a vulnerability and the approach to fixing that vulnerability. Note that Micro Focus does not provide specific code fixes.
    - How to use advanced remediation features of the portal
    - Provide advice and guidance on tuning the results based on organizational policies or specific application coding patterns
- All support provided remotely by suitable qualified personnel. Multiple resources will be used for delivery.

DAST Advanced Support

DAST Advanced Support is available for optional purchase. It is purchased in blocks of 25 person-days effort to be delivered over a 12-month period. DAST Advanced Support is requested through the CSM. 1 weeks' notice is required, and the minimum period is 4 hours.

DAST Advanced Support can be used to assist the Customer in the following areas:

- Scan configuration
  - Scan set-up
  - Macro recording
  - Scan optimization
- Reviewing of scan results
  - Validating coverage
  - False positive suppression
- Results review calls
  - Explain why an issue is being flagged as a vulnerability and the approach to fixing that vulnerability. Note that Micro Focus does not provide specific code fixes.
  - How to use advanced remediation features of the portal
  - Provide advice and guidance on tuning the results based on organizational policies or specific application coding patterns
- All support provided remotely by suitable qualified personnel. Multiple resources will be used for delivery.

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.

Capacity and Performance Management

Fortify Hosted SaaS will be continually monitored for performance issues. Proactive capacity and performance management procedures are in place to ensure the architecture of the environment meets the needs of its Customers.

Operational Change Management

Micro Focus follows a set of standardized methodologies and procedures for efficient and prompt handling of changes to SaaS infrastructure and application, which enables beneficial changes to be made with minimal disruption to the service.

Data Backup and Retention

The data backup and retention described in this section are part of Micro Focus's overall business continuity management practices designed to attempt to recover availability to SaaS and 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
- Fortify Hosted uses this data and produces:
  - Application vulnerability information

In addition, Fortify Hosted stores business contact information for the users of the service. These are typically Customer employees in security and development.

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

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

Disaster Recovery for SaaS

Business Continuity Plan
Micro Focus 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 hours recovery point objective (RPO) and a 24 hours recovery time objective (RTO). 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 AWS Availability Zone in the same AWS Region. 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, (2) validating CHECKSUM at the end of a backup process to assure the same number of bits exists on both source and destination storage systems, and (3) 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 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's continuity plans cover operational shared infrastructure such as remote access, active directory, DNS services, and mail services. Monitoring systems are designed to generate automatic alerts that notify Micro Focus of events such as a server crash or disconnected network.

Controls regarding disruption prevention include:

- Uninterruptible power supplies (UPS) and backup power generators
- At least two independent power supplies in the building
- Robust external network connectivity infrastructure

Data Segregation

Fortify Hosted SaaS is a single tenant architecture. Customer has a dedicated instance of the Fortify Hosted SaaS components and the underlying database instance.

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's standard confidentiality agreement, Micro Focus agrees to respond to a reasonable industry standard information security questionnaire concerning its information and physical security program specific to SaaS no more than once per year. Such information security questionnaire will be considered Micro Focus confidential information.

Micro Focus Security Policies

Micro Focus conducts annual reviews of its policies around the delivery of SAAS against ISO 27001, which includes controls derived from ISO 27034 – "Information Technology – Security Techniques – Application Security". Micro Focus regularly re-evaluates and updates its information and physical security program as the industry evolves, new technologies emerge, or new threats are identified.

Micro Focus Fortify Hosted Information Security Management System is ISO 27001 certified, and the Data Center's used to deliver the Fortify Hosted SaaS hold a Type 2 SOC 2 Report attesting to the adequacy of applicable Trust Services Criteria. A copy of the ISO 27001 certificate and Statement of Applicability (SOA), and the relevant SOC 2 Report can be provided on request.

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 softwaresoc@microfocus.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 Customer 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.

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

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

A two-hour maintenance window once a month starting Monday 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

Micro Focus will apply upgrades to the Fortify software components based on the nature of the associated Fortify product release and in accordance with the internal Micro Focus SaaS update/upgrade policies as defined below.

Upgrade Type	Description	Sandbox Upgrade Term Objective	Production Upgrade Term Objective	Production Notice Period Objective
Release	Upgrade with significant new or improved functionality	2 weeks	3 months	3 months
Patch	Upgrade with corrections or minor enhancements to the product capability of the Release	1 week	1 month	1 month

	that does not change the core functionalities or material features of the product.			
Hotfix	Upgrade with one or more corrections to a Release or Patch	1 week	2 weeks	2 weeks
Security Content	Fortify security rules	1 week	1 month	1 month

Micro Focus will endeavour to notify the Customer of the contents of an upgrade prior to performing the upgrade as per the Production Notice Period define above. The upgrade will be applied initially to the Sandbox environment allowing time for the Customer to test the upgrade ahead of it being applied to the production environment.

The Sandbox Environment will be upgraded within the Sandbox Upgrade Term Objective. The upgrade will be applied to the production environment after the Production Notice Period and within the later of the Production Upgrade Term Objective or the next available Scheduled Maintenance window. If mutually agreed the upgrade can be applied earlier.

Upgrades for all supporting software infrastructure components will be in-line with Micro Focus's ISMS controls.

Service Decommissioning

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

Micro Focus will make available to Customer 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 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 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 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 % ("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 (2,189 actual hours available / 2,200 possible available hours = 99.5% 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

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.

Assessment Time

Customer acknowledges that the time for an individual SAST or DAST assessment to complete is dependent on a range of factors including the size and complexity of the application, volume of assessments being submitted within a given time frame, and the number and configuration of the SAST/DAST Scan Machines. Micro Focus does not provide a Service Level Objective for a particular assessment completing within a specific time.

Standard Service Requirements

Roles and Responsibilities

This section describes general Customer and Micro Focus responsibilities relative to SaaS. Micro Focus's ability to fulfill its responsibilities relative to SaaS is dependent upon Customer fulfilling the responsibilities described below and elsewhere herein:

Customer Roles and Responsibilities

Customer Role	Responsibilities
Business Owner	• Owns the business relationship between the Customer and Micro Focus • Owns the business relationship with the range of departments and organizations using 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 tier-1 support and works with Micro Focus to provide tier-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 Center (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 24x7 application support
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

Micro Focus Fortify Hosted Specific Roles and Responsibilities

Role	Additional Responsibilities
Customer Administrator	• Establishing and maintaining their VPN endpoint Site-to-Site VPN connection or the range of IP addresses that can access the service • Connectivity to internal web applications or APIs for DAST
Customer Subject Matter Expert	• Configuring and running scans • Triaging results • Generating reports • Setting up Fortify End-User Tools

It is a prerequisite for delivery of the Fortify Hosted SaaS solution that the Customer personnel performing the Administrator and Subject Matter Expert role have been trained or are experienced in using Fortify Software Security Center with ScanCentral.

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