

Service Description

Fortify on Demand

United States Public Sector Service

January 2025

Contents

Contents..... 2
Standard Service Features 3
Data Backup and Retention 10
SaaS Security 11
Audit 13
Micro Focus Security Policies..... 13
Security Incident Response..... 14
Micro Focus Employees and Subcontractors 14
Scheduled Maintenance 14
Service Decommissioning..... 15
Service Level Objectives..... 15
Standard Service Requirements..... 17

This Service Description describes the components and services included in 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.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

Fortify on Demand (FoD) for United States Public Sector is a remotely delivered, cloud-based application security as a service solution. With its FedRAMP authorization, FoD allows government agencies to perform security assessments regardless of where the application resides and without any software to install or manage.

Application security testing is performed and reviewed by application security experts using application testing technologies and manual techniques. All customers are provided access to our technical account support team.

FoD provides static, dynamic website, and dynamic API application security assessments. For each single assessment or subscription requested, the customer chooses a combination of one assessment type and service level for one (1) application. The customer may access reports which detail the findings of the assessment(s) in a standard FoD format by accessing the FoD web application portal. FoD also offers open- source software composition analysis and supplemental support services.

SaaS Delivery Components

SaaS Delivery Components

One Fortify on Demand production tenant hosted in Fortify on Demand FedRAMP environment	✓
✓ = Included	
○ = Optional for a fee	

SaaS Operational Services

Fortify on Demand (FoD) Operational Services include a range of options for assessments and support, as purchased, all of which are described below. FoD static, dynamic website, dynamic, dynamic API and mobile application security assessments are made available by purchasing and redeeming FoD Assessment Units (AUs). AUs are pre-paid credits that are redeemed for a single assessment or a single application subscription and are valid for the lesser of twelve (12) months from the effective date of the SaaS Order Term or the term referenced on the legal quote.

A customer may purchase up to three (3) years of AUs on a single purchase 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 subscription allows for one application to be assessed an unlimited number of times during a twelve-month term beginning at the beginning of the applicable SaaS Order Term (Subscription Term). For a multi-year purchase, the Subscription Term is the twelve (12) month period beginning on the issue date for the AUs redeemed for that application subscription. Applications cannot be swapped out during the Subscription Term.

Assessment Type	Single Assessment	Subscription
Static Assessment	N/A	4 Assessment Units
Static+ Assessment	2 Assessment Units	6 Assessment Units
Static NCD Subscription	n/a	16 Assessment Units per 10 NCDs
Dynamic Website Assessment	3 Assessment Units	9 Assessment Units
Dynamic API Assessment	3 Assessment Units	9 Assessment Units
Debricked Assessment	n/a	1 Debricked Assessment Unit
Debricked NCD Subscription	Not Applicable	5 Debricked Assessment Units per 10 Debricked NCDs

Static Application Security Assessment (Named Contributing Developer (NCD) Subscription)

A **Named Contributing Developer** (NCD) is 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 Named Contributing Developers may be assessed. For the avoidance of doubt, at least one (1) Contributing Developer license is required for each application.

Micro Focus will perform unlimited Static Assessments of the code developed by Named Contributing Developers during the Subscription Term. A Static Assessment consists of the following activities:

- Perform static code analysis using Micro Focus Fortify Static Code Analyzer (SCA) of the application source, byte and/or binary code uploaded by the Customer
- Automated audit of prioritized results to remove false positives using Micro Focus Fortify Audit Assistant

Static Application Security Assessment (Subscription)

Recommended for individual applications subject to ongoing development activity, managed development teams participating in uniform SDLC integration and skilled source code security audit support. Micro Focus will perform unlimited Static Assessments during the Subscription Term. Only one assessment can be active at any time. If an assessment is already running when a new assessment is submitted, it can be queued. A Static Assessment consists of the following activities:

- Perform static code analysis using Fortify SCA of the application source, byte and/or binary code uploaded by the Customer
- For the initial assessment, Micro Focus will provide a review of prioritized results by a FoD security expert including false positive removal
- For all subsequent assessments during the Subscription Term, Micro Focus will provide an automated audit of prioritized results using the standard FoD issue template

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. Microservice applications do not include a review by a FoD security expert on the initial assessment; all Static Application Security Assessments of a microservice application include an automated audit using the standard FoD issue template.

Static+ Application Security Assessment (Single Assessment)

Recommended for baseline audits of application portfolios as well as baseline/update audits for individual applications subject to periodic development activity (examples: legacy or maintenance applications). Micro Focus will perform a single Static+ Assessment which consists of the following activities:

- Perform static code analysis using Fortify SCA of the application source, byte and/or binary code uploaded by the Customer
- Review of prioritized results by a FoD security expert including false positive removal
- One (1) remediation validation within thirty (30) days of the assessment

Static+ Application Security Assessment (Subscription)

Recommended for individual applications subject to ongoing development activity, managed development teams separate from uniform SDLC integration and/or without skilled source code security. audit support. Micro Focus will perform unlimited Static+ Assessments during the Subscription Term. Only one assessment can be active at any time. If an assessment is already running when a new assessment is submitted, it can be queued. A Static+ Assessment consists of the following activities:

- Perform static code analysis using Fortify SCA of the application source, byte and/or binary code uploaded by the Customer
- For up to twelve (12) assessments during the Subscription Term, Micro Focus will provide a review of prioritized results by a FoD security expert including false positive removal
- For all other assessments during the Subscription Term, Micro Focus will provide an automated audit of prioritized results to remove false positives using the standard FoD issue template

Dynamic Website Application Security Assessment (Single Assessment)

Micro Focus will perform a single Dynamic Web Assessment which consists of the following activities:

- Verify URL and credentials of web application to be assessed
- Perform an automated, authenticated Micro Focus Fortify WebInspect assessment of the web application
- Review of prioritized results by a FoD security expert including false positive removal
- One (1) remediation validation within thirty (30) days of the assessment

Dynamic Website Application Security Assessment (Subscription)

Micro Focus will perform unlimited Dynamic Web Assessments during the Subscription Term. Only one assessment can be active at any time. A Dynamic Web Assessment consists of the following activities:

- Verify URL and credentials of web application to be assessed
- Perform an automated, authenticated WebInspect assessment of the web application
- Review of prioritized results by a FoD security expert including false positive removal

Dynamic API Application Security Assessment (Single Assessment)

Micro Focus will perform a single Dynamic API Assessment which consists of the following activities:

- Verify the API URL and customer provided OpenAPI JSON specification or Postman collection that describes API endpoints to be assessed
- Perform an automated WebInspect assessment of designated API endpoints using customer provided OpenAPI JSON specification or Postman collection
- Review of prioritized results by a FoD security expert including false positive removal
- One (1) remediation validation within thirty (30) days of the assessment

Dynamic API Application Security Assessment (Subscription)

Micro Focus will perform unlimited Dynamic API Assessments during the Subscription Term. Only one assessment can be active at any time. A Dynamic API Assessment consists of the following activities:

- Verify the API URL and customer provided OpenAPI JSON specification or Postman collection that describes API endpoints to be assessed
- Perform an automated WebInspect assessment of designated API endpoints using customer provided OpenAPI JSON specification or Postman collection

Debricked Assessment Subscriptions

Debricked Assessment Subscription allows the customer to perform automated software composition analysis to identify open-source components and other third-party software that is present in an application. The results of a Debricked Assessment include the Software bill-of-materials (SBOM) along with security issues and license information associated with the identified components.

A Debricked Assessment Subscription allows for one application to be assessed an unlimited number of times during the Subscription Term. The Subscription Term is the lesser of twelve (12) months from the effective date of the SaaS Order Term or the term referenced on the legal quote. Applications cannot be swapped out during the Subscription Term.

A Debricked Named Contributing Developer (Debricked NCD) Subscription allows for unlimited assessments of application developed by Debricked NCDs during the Subscription Term. Customer may use Debricked scans with Static Scans or independently, depending on Customer need, subject to remaining Assessment Units.

Architecture Components

Fortify on Demand (FoD) 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. FoD 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. Customer must have internet connectivity to access FoD. No components or software are required for installation on the customer premise to facilitate application testing or result consumption.

FoD static, dynamic website, dynamic, dynamic API and mobile application security assessments are made available by purchasing and redeeming FoD Assessment Units (AUs). AUs are pre-paid credits that are redeemed for a single assessment or a single application subscription and are valid for the lesser of twelve (12) months from the effective date of the SaaS Order Term or the term referenced on the legal quote.

Application Administration

Static Assessments

For static assessments, a Customer may only use an application that meets the Fortify SCA minimum requirements for currently supported languages, which should be successfully compiled prior to submission of the application. An application is defined as a deployable unit of code consisting of a collection of source and/or byte code instruction files that:

- Can deliver some or all the functionality of a business application
- Is written in the same technology family
- Is built on a single platform
- Does not include any loosely coupled components
- Can be configured to run on an application server (e.g., a Web Application Archive [WAR] or Enterprise Archive [EAR] file for a Java application or a solution in team foundation server 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.

Dynamic website and API assessments

For all dynamic website and API 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
- www.example.com/news/ is the same hostname and hence the same FQDN and so is the same application
- community.example.com is a different subdomain and hence a different FQDN and so is a different application
- www.example.co.uk is a different domain name and hence a different FQDN and so is a different application

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

- Forms authentication and single network authentication (basic/digest/NTLM) is allowed
- Forms authentication, single network authentication and application generated authentication such as bearer tokens is allowed

User logins may not be “daisy chained”. For example, two Forms authentication mechanisms are not permitted.

For API applications only, the customer must provide a definition of the API endpoints:

- 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 values for all parameters, must be provided

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 FoD testing team using IP whitelisting and/or site-to-site VPN. Customer must confirm that the web 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 anti-automation technology or whitelist

Micro Focus to perform a more comprehensive dynamic assessment. If Customer chooses or is not able to disable the anti-automation technology, coverage of the WebInspect assessment may be reduced, such as by performing an unauthenticated assessment if MFA is enabled or not assessing functionality blocked by CAPTCHA.

Debricked Assessments

Debricked Assessments may only be conducted in conjunction with a FoD static assessment; therefore, the application definition for static assessments applies to all Debricked Assessments. Customer must include Debricked-supported manifest file(s) in the uploaded ZIP file.

Service Support

Operational Support Services	Standard Support	Managed Support	Enhanced Support	Premium Support	Add-On Support Packages
Welcome Pack	◆	◆	◆	◆	
Self Service Portal	◆	◆	◆	◆	
Help Desk Support	◆	◆	◆	◆	
Nominated Technical Account Manager		◆	◆	◆	◆
Onboarding Development Team		1st	4	All	1st
Results Review Calls			2 per month	8 per month	4 per month
Integration Support			1	All	
Nominated App Sec Program Manager				◆	
App Sec Program Support				◆	
Customized Training Support				◆	
Additional Notes	Included	Included if >100 AU's are purchased	Annual Fixed Fee	Annual Fixed Fee	Purchased Individually

Standard Support

Standard Support is included with all purchases. The Customer may contact Micro Focus through email or telephone. 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 and resolution time. Online support and product documentation are available within the FoD web portal.

- Micro Focus staffs and maintains a Service Operations Center, which will be the single point of

contact for all issues related to the support for FoD service for the Customer. The Customer will maintain a list of authorized users who may contact Micro Focus for support. The Customer's authorized users may contact Micro Focus for support via web portal, email at FoD-FedRAMP-Support@microfocus.com or telephone the Service Operations Center during standard business hours (US Eastern Time Zone, 9 hours a day, 5 days a week).

- Instructional emails and a recorded demo of the Fortify on Demand portal
- All support is provided remotely by United States citizens

Managed Support

Managed Support is included for all purchases of more than one hundred (100) AUs. Managed Support is also available for optional purchase if the customer purchases less than one hundred (100) AUs. The Customer receives all the features of Standard Support in addition to the following:

- Customer is assigned a Customer Manager (CM) as a primary point of contact
 - CM is a shared resource
 - CM is a United States citizen
- On-boarding first development team
 - Live Portal Walk-thru – One (1) hour session
- Applications section, dashboard section, report section, administration section, training section, support section (how to videos, documentation, on-line chat)
- Additional training sessions can be purchased
 - Live integration tools walk-thru – One (1) hour session
- Provides an overview of the integration tools and the API
- Guidance for integrating FoD into the customers development toolchain including build server and IDE's
 - Results walk- thru of the first scan completed in FoD – One (1) hour session
- 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 CM
 - These calls will include review of scanning activity, entitlement consumption and provide best practice guidance
- Manage service requests, such as support and maintenance services or issues regarding availability of the FoD infrastructure technical support
- All support provided remotely

Enhanced Support

The Enhanced Support service is available for optional purchase. The Customer receives all the features of Managed Support in addition to the following:

- On-board Development Teams increased from one (1) to four (4)
- Integration Support for one custom integration
 - One (1) hour 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 FoD API to develop integration
- Results review calls
 - Up to two (2) one (1) hour calls per month with client security and development teams to review scan results

- Explain why an issue is being flagged as a vulnerability and the approach to fixing that vulnerability. Note that we don't 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

Premium Support

The Premium Support service is available for optional purchase. The Customer receives all the features of Enhanced Support in addition to the following:

- Customer is assigned an Application Security Program Manager (ASPM)
 - Available during assigned resources standard business hours
 - ASPM is a shared resource
 - ASPM is a United States citizen
- AppSec Program Support
 - Program kickoff, milestone and AppSec goal planning
 - Share current AppSec best practices
 - Assist the client AppSec team with leveraging FoD in their organization
- Assists client's technical writer in preparing customized FoD training
- On-board development teams increased from four (4) to unlimited
- Results review calls increased from up to two (2) per month to up to eight (8) per month
- Integration support increased from one (1) to unlimited custom integrations.
- One (1) on-site visit per year as necessary

Results Review Calls

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

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 FoD 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'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 on Demand uses this data and produces:
 - Application vulnerability information

In addition, Fortify on Demand 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) 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. Micro Focus's FoD for United States Public Sector SaaS environment meets all security requirements for certification as a FedRAMP moderate level SaaS solution.

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'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

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.

The Joint Authorization Board (JAB) of the Federal Risk and Authorization Management Program (FedRAMP) has completed the review of the FoD for United States Public Sector. Based on the Federal Information Processing Standard (FIPS) security categorization of "Moderate" (Confidentiality=Moderate, Integrity=Moderate, Availability=Low) and the FedRAMP Security Assessment Process, the JAB determined the Micro Focus USPS system meets the information security requirements and has been granted a FedRAMP Provisional Authorization (P-ATO).

The JAB provides guidance for FoD to assist in determining the scope of an annual assessment based on NIST SP 800-53, FedRAMP baseline security requirements, and FedRAMP continuous monitoring requirements.

The security authorization will remain in effect for a length of time in alignment with Office of Management and Budget Circular A-130, as long as:

- FoD for United States Public Sector satisfies the requirement of implementing continuous monitoring activities as documented in FedRAMP's continuous monitoring requirements

- FoD for United States Public Sector mitigates all open low and moderate POA&M action items, agreed to in the Security Assessment Report (SAR)
- Significant changes or critical vulnerabilities are identified and managed in accordance with applicable Federal law, guidelines, and policies

For additional information, visit fedramp.gov.

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. Micro Focus employees, affiliates and subcontractors involved in the processing of Customer-provided SaaS Data meet all US citizenship requirements specified by FedRAMP program rules, are bound by appropriate confidentiality obligations, and have undergone all training required to meet FedRAMP moderate level controls.

Scheduled Maintenance

To enable Customers to plan for scheduled maintenance by Micro Focus, Micro Focus reserves predefined timeframes to be used on an as-needed basis. Micro Focus reserves a weekly two (2) hour window (Thursday 00:00 to 02:00 US Eastern Time Zone) and one (1) monthly twenty-four (24) hour window (Saturday 00:00 to Sunday 00:00 US Eastern Time Zone). These windows will be used on an as-needed basis.

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. SaaS Upgrades are evaluated in accordance with the rules of the FedRAMP program prior to release.

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 hereinto 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'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 (2,198 actual hours available / 2,200 possible available hours = 99.9% availability).

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

Boundaries and Exclusions

Solution Uptime shall not apply to or include any time during which SaaS is unavailable in connection with any

of the following (specifically, the number of hours of unavailability in the measured period per the Measurement Method section above due to the following shall not be included in either the numerator or the denominator for the measurement):

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g., DNS servers) due to virus or hacker attacks
- Force majeure events
- Actions or omissions of Customer (unless undertaken at the express direction of Micro Focus) or third parties beyond the control of Micro Focus
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Micro Focus
- Scheduled maintenance
- Scheduled SaaS upgrades

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 FoD solution. 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 FoD security experts about the application. Micro Focus targets to deliver 95% of assessments within the Security Assessment Time for each assessment type.

Due to United States citizenship requirements of the FedRAMP program, the Security Assessment Time SLO represent a target time frame and cannot be guaranteed.

Assessment Type	Automated Audit	Security Expert Review
Static Assessment	Four (4) hours	Two (2) days
Static+ Assessment	Four (4) hours	Two (2) days
Dynamic Website Assessment	N/A	Two (2) days
Dynamic API Assessment	N/A	Two (2) days

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

- Application has not been packaged correctly as per FoD best practice guidelines
- The application payload exceeds 1,000MB

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

- FoD is not provided continuous 24-hour per day access and fully operational test credentials to assess the application that is in scope
- FoD is not able 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

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. Initial SaaS Response will come as an email to the requester. The Initial SaaS Response Time covers both service request and support requests. Micro Focus targets to provide the

Initial SaaS Response no more than twenty-four (24) hours, excluding weekends 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’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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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
<p>Customer Service Center (CSC)</p>	<ul style="list-style-type: none"> • 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 the availability of SaaS • Provides 9x5 application support
<p>Operations Staff (Ops)</p>	<ul style="list-style-type: none"> • 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 9x5 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 Fortify on Demand 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 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
- Customer is responsible for their Authority to Operate (ATO). Based on the documentation within the FedRAMP secure repository and customer-specific tailoring and operating procedures, separate Federal Agencies should seek their own security authorization package, which accurately documents the FoD for United States Public Sector and clearly defines outstanding risk considerations.

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

Service Description
Fortify on Demand (FedRAMP)

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'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.