Service Description

Fortify on Demand

Standard Service

February 2021

MICRO FOCUS

Contents

This Service Description describes the components and services included in Micro Focus Fortify on Demand (which also may be referred to as "SaaS"). Unless otherwise agreed to in writing this Service Description is subject to the Micro Focus Customer Terms for Software-as-a-Service or the applicable Micro Focus Pass-Through Terms and represents the only binding terms governing Micro Focus International PLC and its affiliates ("Micro Focus") respective obligations regarding its provision of this SaaS to the end-user customer.
Any other descriptions of the features and functions of the SaaS, public statements, including advertisements, shall not be deemed as additional features or functionalities that Micro Focus is required to deliver.

Standard Service Features

High Level Summary

Fortify on Demand (FoD) is a remotely-delivered, cloud-based application security as a service solution. 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, dynamic web services and mobile 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, computer-based secure development training, and supplemental support services.

Application Security Assessments

FoD static, dynamic website, dynamic, dynamic web services 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 are 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	1 Assessment Unit	4 Assessment Units
Static+ Assessment	2 Assessment Units	6 Assessment Units
Dynamic Website Assessment	2 Assessment Units	6 Assessment Units
Dynamic+ Website Assessment	6 Assessment Units	18 Assessment Units
Dynamic Web Services Assessment	2 Assessment Units	6 Assessment Units
Dynamic+ Web Services Assessment	6 Assessment Units	N/A
Mobile Assessment	1 Assessment Unit	4 Assessment Units
Mobile+ Assessment	6 Assessment Units	18 Assessment Units

Static Application Security Assessment (Single Assessment)
Micro Focus will perform a single Static Assessment which 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 Scan Analytics
- One (1) remediation validation within thirty (30) days of the assessment

Static Application Security Assessment (Subscription)
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 one (1) assessment, Micro Focus will provide a review of prioritized results by a FoD security expert including false positive removal (typically the initial assessment)
- For all subsequent assessments during the Subscription Term, Micro Focus will provide an automated audit of prioritized results to remove false positives using Fortify Scan Analytics

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 Fortify Scan Analytics.

Static+ Application Security Assessment (Single Assessment)
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)
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 each assessment, Customer may choose one (1) of the following:
    - Review of prioritized results by a FoD security expert including false positive removal
    - Automated audit of prioritized results to remove false positives using Fortify Scan Analytics

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

The Dynamic Website Assessment Subscription also includes Continuous Application Monitoring automated, unauthenticated dynamic vulnerability assessments up to four times per month for the web application.

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 WebInspect assessment of the web application
- Manually assess the target web application using the FoD testing methodology
- Includes up to eight (8) hours of analysis by a FoD security expert
- 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
    - Manually assess the target web application using the FoD testing methodology
- Includes up to eight (8) hours of analysis by a FoD security expert
- Review of prioritized results by a FoD security expert including false positive removal

The Dynamic+ Website Assessment Subscription also includes Continuous Application Monitoring automated, unauthenticated dynamic vulnerability assessments up to four times per month for the web application.

Dynamic Web Services Application Security Assessment (Single Assessment)
Micro Focus will perform a single Dynamic Web Services Assessment which consists of the following activities:

- Verify the Web Service URL and customer-provided OpenAPI JSON specification or Postman collection that describes web service endpoints to be assessed
- Perform an automated WebInspect assessment of designated web service 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 Web Services Application Security Assessment (Subscription)
Micro Focus will perform unlimited Dynamic Web Services Assessments during the Subscription Term. Only one assessment can be active at any time. A Dynamic Web Services Assessment consists of the following activities:

- Verify the Web Service URL and customer-provided OpenAPI JSON specification or Postman collection that describes web service endpoints to be assessed
- Perform an automated WebInspect assessment of designated web service endpoints using customer-provided OpenAPI JSON specification or Postman collection
- Review of prioritized results by a FoD security expert including false positive removal

Dynamic+ Web Services Application Security Assessment (Single Assessment)
Micro Focus will perform a single Dynamic+ Web Services Assessment which consists of the following activities:

- Verify the Web Service URL, credentials, and Customer-provided definition of web service endpoints to be assessed
- Perform an automated, authenticated WebInspect assessment of designated web service endpoints
- Manually assess the target web service endpoints using the FoD testing methodology
    - Includes up to eight (8) hours of analysis by a FoD security expert
- Review of prioritized results by a FoD security expert including false positive removal
- One (1) remediation validation within thirty (30) days of the assessment

Mobile Application Security Assessment (Single Assessment)
Micro Focus will perform a single Mobile Assessment which consists of the following activities:

- Perform vulnerability analysis of the mobile application client iOS or Android binary uploaded by the Customer
- Perform reputation analysis for any discovered URL endpoints
- Review of prioritized results by a FoD security expert including false positive removal
- One (1) remediation validation within thirty (30) days of the assessment

Mobile Application Security Assessment (Subscription)
Micro Focus will perform unlimited Mobile Assessments during the Subscription Term. Only one assessment can be active at any time. A Mobile Assessment consists of the following activities:

- Perform vulnerability analysis of the mobile application client iOS or Android binary uploaded by the Customer
- Perform reputation analysis for any discovered URL endpoints
- Review of prioritized results by a FoD security expert including false positive removal

Mobile+ Application Security Assessment (Single Assessment)
Micro Focus will perform a single Mobile+ Assessment which consists of the following activities:

- Perform vulnerability analysis of the mobile application client iOS or Android binary uploaded by the Customer
- Perform reputation analysis for any discovered URL endpoints
- Perform an automated, authenticated WebInspect assessment of Customer-owned web service endpoints
- Manually assess the mobile application binary, network and server layers using the FoD testing methodology
    - Includes up to eight (8) hours of analysis by a FoD security expert
- Review of prioritized results by a FoD security expert including false positive removal
- One (1) remediation validation within thirty (30) days of the assessment

Mobile+ Application Security Assessment (Subscription)
Micro Focus will perform unlimited Mobile+ Assessments for the Subscription Term. Only one assessment can be active at any time. A Mobile+ Assessment consists of the following activities:

- Perform vulnerability analysis of the mobile application client iOS or Android binary uploaded by the Customer
- Perform reputation analysis for any discovered URL endpoints

- Perform an automated, authenticated WebInspect assessment of Customer-owned web service endpoints
- Manually assess the mobile application binary, network and server layers using the FoD testing methodology
    - Includes up to eight (8) hours of analysis by a FoD security expert
- Review of prioritized results by a FoD security expert including false positive removal

Sonatype Assessment Subscriptions

Sonatype Assessments Subscriptions utilize automated analysis powered by Sonatype to identify open source components and other third-party software that is present in an application. The results of a Sonatype Assessment include the third-party component bill-of-materials along with security issues and license information associated with the identified components.
A Sonatype 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.
Sonatype Assessments may only be requested in conjunction with a FoD Static or Static+ Assessment using the same application source, byte and/or binary code uploaded by the Customer for the FoD Static or Static+ Assessment. Supported languages and frameworks for Sonatype Assessments are based on the capabilities provided by Sonatype, which may differ from the languages and frameworks supported by Fortify SCA for the associated FoD Static or Static+ Assessment. Application code uploaded by the Customer is analyzed in the FoD datacenter and is not transmitted to or accessed by Sonatype as part of a Sonatype Assessment.

Computer-based Training

Micro Focus will provide Customer access to its Micro Focus Fortify-branded Application Security Computer-Based Training courses (CBTs) via FoD with the purchase of CBT Training. Access is for a named user for a twelve (12) month period to a specific role-based Standard or Premium course curriculum.
The following criteria shall apply to these CBT courses:

- A named user shall be classified as a specific individual with a unique email address.
- One (1) registered email address shall use one (1) license count for access to the courses in the Application Security Training Course List.
- Accounts shall not be shared.
- All CBTs are valid for a twelve (12) month period. Any unused CBTs shall expire after this period and are not eligible for carryforward or credit.

Customer does not have to specify up-front the exact course curricula required. Customer cannot exchange individual courses within a course curriculum for other courses in another course curriculum. Course content is provided through the Micro Focus partnership with Security Innovation. Micro Focus may substitute individual courses within a curriculum with substantially equivalent courses as new course content is made available by Security Innovation.

Architecture Components

FoD consists of cloud-based interactive management web-based 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.

Service Support Options

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 a variety of methods such as online chat, support tickets, 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 24x7x365 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 the web portal or telephone at +1 800 893 8141, 24 hours a day, 7 days a week.
- Instructional emails and a recorded demo of the Fortify on Demand portal
- All support is provided remotely.

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 Technical Account Manager (TAM) as a primary point of contact
    - TAM is a shared resource
- 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 held 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 TAM
    - 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 to
        - 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
- 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.

Application Administration

A SaaS Order Term is valid for a single application deployment, which cannot be changed during the SaaS Order Term. A subscription is valid for a single application, which cannot be changed during the subscription term purchased.

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.

Static assessments

For static assessments, an application must meet the Fortify SCA minimum requirements for currently supported languages and be able to 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 of 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 of 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 web services assessments

For dynamic assessments, an application is defined as a fully qualified domain name (FQDN) and has a single authentication management system. User logins may not be "daisy chained" within the application. The application must be the same hostname:

- www.microfocus.com is a hostname
- www.microfocus.com/news/ is the same host as www.microfocus.com
- community.microfocus.com is a different hostname and is considered a different application
- www.microfocus.co.uk is a different hostname and is considered a different application

For REST web services applications, an endpoint is a combination of a URI and HTTP method. All endpoints in the application must be for the same FQDN. For example, the following endpoints are a single application:

- GET https://api.microfocus.com/api/v1/Accounts
- GET https://api.microfocus.com/api/v1/Accounts/{AccountId}
- PUT https://api.microfocus.com/api/v1/Accounts/{AccountId}
- GET https://api.microfocus.com/api/v2/orders/{orderId}/items/{itemId}
- POST https://api.microfocus.com/api/v2/orders/{orderId}/items/{itemId}

For SOAP web services applications, an endpoint is an individual method provided by a web service. All endpoints in the application must be defined in a single SOAP WSDL file. In the WSDL, the service is indicated by the <service> tag and the method by the <operation> tag.

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 in order 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. On a Dynamic+ Assessment, manual testing supports email one-time-password (OTP) when assessing applications with MFA. Micro Focus, at its sole discretion, may attempt to support other MFA technology, such as SMS OTP,

for manual testing performed during a Dynamic+ assessments.

Any cancellations or delays of more than two (2) hours require 24-hour notice prior to the scheduled assessment. The Customer may be required to confirm authorization to perform a security assessment of the application. Micro Focus is not liable for any monetary or technical damages as a result of the assessment on the requested URL.

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

Sonatype Assessments
Sonatype Assessments may only be conducted in conjunction with a FoD static assessment; therefore, the application definition for static assessments applies to all Sonatype Assessments.

Service Components

Service Monitoring

Micro Focus monitors FoD solution components for 24x7 availability. Micro Focus uses a centralized notification system to deliver proactive communications about application changes, outages and scheduled maintenance. Alerts and notifications are available to the Customer via the FoD portal.

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. Changes to production environments are reviewed via an internal Change Advisory Board (CAB), prior to implementation to ensure they are appropriately scheduled and tested before promotion to production.

Solution 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 Customer of FoD and access to the FoD Customer data, following an outage or similar loss of service.

The Data Backup Frequency is one (1) day and Micro Focus performs that daily backup of the FoD database (including configuration data). The Backup Retention Time is fourteen (14) days, meaning Micro Focus retains each daily backup for the most recent fourteen (14) days ("Backup Retention Time").

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.

In some regions, Fortify on Demand is implemented over an AWS or Azure technology service stack in a redundant mode over two Availability zones (AZs) with elastic load balancing. Availability zones (AZs) are distinct geographical locations that are engineered to be insulated from failures in other AZs. Elastic IP addresses are used to work around host or availability zone failures.

Disaster Recovery

Business Continuity Plan

Micro Focus continuously evaluates different risks that might affect the integrity and availability of the FoD solution. 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 plain ("DRP"). Micro Focus utilizes the BCP to provide core FoD solution and infrastructure services with minimum disruption. The DRP includes a set of processes that Micro Focus implements and tests FoD 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). 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 at a remote site. Micro Focus uses storage and database replication for its remote site backup process. The integrity of backups are 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 Customer Personal Data and confidential information (the "Micro Focus Security Program").

Technical and Organizational Measures

This section describes Micro Focus´s standard technical and organizational measures, controls and procedures, which are intended to help protect the Customer-provided SaaS Data. 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;
- securing equipment hosting Customer-provided SaaS Data in designated caged areas; and
- maintaining an audit trail of access.

Access Controls

Micro Focus maintains the following standards for access controls and administration designed to make Customer-provided 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;
- Customer provided 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 Micro Focus SaaS environment;
- collection and maintenance of log audits for the application, OS, DB, network and security devices according to the baseline requirements identified;
- restriction of access to log information based on user roles and the "need-to-know;" and
- prohibition of shared accounts.

Availability Controls

Micro Focus´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; and
- robust external network connectivity infrastructure.

Data Segregation

Micro Focus SaaS environments are segregated logically by Micro Focus 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 Customer-provided SaaS Data in transit and at rest. 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 the applicable FoD solution. A summary report or similar documentation will be provided to Customer upon request. Subject to the 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 Micro Focus SaaS provided pursuant to the applicable Supporting Material no more than once per year. Alternatively, a copy of Micro Focus's Cloud Security Alliance Consensus Assessment Initiative Questionnaire (CAIQ) v3. 1 self-assessment can be provided on request. Such information security questionnaires will be considered Micro Focus Confidential Information.

Micro Focus Security Certifications

Micro Focus conducts annual reviews of its policies around the delivery of SaaS against ISO 27001. 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 on Demand's Information Security Management System is ISO 27001 certified and the Data Center's used to deliver the FoD Service 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 Customer-provided SaaS Data ("Security Incident"), Micro Focus will notify Customer of the Security Incident and work to 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 email at swpmb.softwaresoc@microfocus.com.

Micro Focus Employees and Subcontractors

Micro Focus requests that all employees involved in the processing of Customer-provided SaaS Data are authorized personnel with a need to access the Customer-provided SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of customer data. Micro Focus requests that any affiliate or third party subcontractor involved in supporting service delivery 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.

Customer-provided SaaS Data

All data provided to FoD will be considered Customer-provided SaaS Data per the Micro Focus Customer SaaS Terms. Customer will be responsible for all data cleansing and data accuracy as part of any assessment request. Micro Focus is not responsible for the accuracy of the data provided by the customer.

Customer Personal Information - Data Processing Terms

Customer Personnel Information will be processed as per the data processing terms specified in "Section 7. Personal Information" of the Micro Focus Customer Terms for Software-as-a-Service unless otherwise agreed in writing. FoD uses Customer Personal Information as follows:

- Data Subjects
  Authorized users of the service as specified by the customer. These are typically customer employees in security and development.
- Personal Data
  First name, last name, email address, locale, IP address and telephone number (optional)
- Purpose
  The data is only used for the purpose of delivering the FoD service namely authentication, notification of application level events, traceability of application level events and security event logs.
- Data Storage
  Customer can choose the FoD data center where their data will be stored. Available FoD data centers include AMS (United States), EMEA (United Kingdom) and APAC (Australia). All customer data remains in the chosen data center or its back-up facility that is located in the same country.
- Data Processing
  Data is processed in various Micro Focus locations including USA and Philippines. Data is only processed by employees or contingent workers of Micro Focus International PLC or one of its subsidiaries.
- Data Controller
  The Customer remains the Data Controller.

There is no requirement for Micro Focus to have access to any other Customer Personal Information including Personal Health Information or other special categories data as defined by GDPR.

Micro Focus will, within three (3) business days of receipt, refer to Customer any queries from data subjects in connection with Customer Personal Information.

Permitted Uses

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

Micro Focus owns all rights to any data generated by Micro Focus during the course of delivering the FoD services ("Metadata"). Metadata further includes, without limitation, data generated through the Fortify Scan Analytics 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 is managed by the Customer and can be deleted using features of the FoD 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 thirty (30) days. Data is securely deleted from the backup media in accordance with the Backup Retention Time after data is deleted from the FoD service.

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 in the local time zone of the FoD datacenter) and one (1) monthly twenty-four (24) hour window (Saturday 00:00 to Sunday 00:00 in the local time zone of the FoD datacenter). These windows will be used on an as-needed basis.

FoD Datacenter	Local Time Zone
AMS	US Eastern Time Zone
EMEA	Greenwich Mean Time Zone
APAC	Australian Eastern Time Zone

Scheduled Version Updates

"SaaS Upgrades" are defined as both major version updates, minor version updates and binary patches applied by Micro Focus to the FoD solution 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 as part of FoD service unless the SaaS Upgrade introduces new functionality that Micro Focus offers on an optional basis for an additional fee.

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 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 the FoD solution.

Service Decommissioning

Customer may cancel Micro Focus SaaS by providing Micro Focus with sixty (60) days written notice prior to the expiration of the SaaS Order Term ("Cancellation"). Such Cancellation shall be effective upon the last day of the then current SaaS Order Term. Upon Cancellation, expiration, or termination of the SaaS Order Term, Micro Focus may disable all Customer access to FoD solution, 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 such data in the format generally provided by Micro Focus. The target timeframe is set forth below in the Termination Data Retrieval Period SLO section. 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 the services that SaaS provides to its customers. 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 always meet these objectives.

Solution Provisioning Time SLO

Solution Provisioning is defined as the FoD solution being available for access over the internet. Micro Focus targets to make FoD available within five (5) business days of the customer's purchase order (PO) being booked within the Micro Focus order management system. Customer is responsible for installing and configuring any additional onsite components for his applications. Any onsite 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 FoD production application being available for access and use by Customer and its Authorized Users over the Internet. Micro Focus will provide Customer access to the FoD production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99.5 % ("Solution Uptime").

Measurement Method
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 (2189 actual hours available / 2200 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 any of the following exceptions:

- Overall Internet congestion, slowdown, or unavailability
- Unavailability of generic Internet services (e.g. DNS servers) due to virus or hacker attacks
- Force majeure events as described in the terms of the SaaS agreement
- 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 Version Updates

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.

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
Dynamic Website Assessment	N/A	Two (2) days
Dynamic+ Website Assessment	N/A	Three (3) days
Dynamic Web Services Assessment	N/A	Two (2) days
Dynamic+ Web Services 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)"

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 and Mobile 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
- Mobile binary is obfuscated or is not prepared as per FoD best practice guidelines

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the Service Support described herein. It is defined as the acknowledgment of the receipt of a customer 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 a customer 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 Customer FoD data from Micro Focus. Micro Focus targets to make available such data for download in the FoD format generally provided by Micro Focus for thirty (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 the FoD solution. 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 the FoD solution • 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 FoD solution end users for problem isolation • Performs FoD solution 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 FoD solution administrators • Provides periodic feedback to the FoD solution Administrator

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Customer Success Manager (CSM)	• Serves as the customer liaison to Micro Focus • Coordinates Micro Focus resources including system and process experts as necessary • Facilitates ongoing mentoring • Coordinates with the customer during required and periodic maintenance • Oversees the customer onboarding process

Service Operations Center staff (SOC)	• 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 the FoD solution • Provides 24x7 application support
Operations staff (Ops)	• Monitors the FoD solution for availability • Provides 24x7 SaaS infrastructure and application support • Performs system-related tasks such as backups, archiving, and restoring instances according to Micro Focus's standard practices

Assumptions and Dependencies

This Service Description is based upon the following assumptions and dependencies between the Customer and Micro Focus:

- The service commencement date is the date on which Customer´s purchase order (PO) is booked within the Micro Focus order management system.
- Customer must ensure that its administrators maintain accurate contact information with FoD.
- 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 the FoD solution is provided based on the assumption that Customer will implement and maintain the following controls in its use of FoD:

- Configuring Customer's browser and other clients to interact with the FoD solution
- Configuring Customer's network devices to access the FoD solution
- Appointing authorized users
- Configuring its FoD 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 perform the 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.