
Service Description

Service Description

Debricked on Software-as-a-Service

August 2023



Copyright 2023 Open Text

V7.4

Contents

Contents 2
Standard Service Features..... 3
Data Backup and Retention 5
SaaS Security 6
Audit 7
Micro Focus Security Policies 8
Security Incident Response 8
Micro Focus Employees and Subcontractors 8
Data Subject Requests 8
Service Decommissioning..... 8
Service Level Objectives 8
Standard Service Requirements..... 10

This Service Description describes the components and services included Debricked SCA on Software-as-a-Service (which also may be referred to as “Debricked” or “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

The Debricked SCA tool is a remotely delivered, cloud-based Software Composition Analysis as a service solution. Third-party component risk scans are performed automatically on push or merge events in the Customer's CI/CD pipeline.

The Debricked SCA tool provides Software Bill of Materials (SBOM) creation, vulnerability scanning, license compliance scanning and community health scanning of all third-party components present in the Customer's dependency/manifest files. The Customer may access the results through output in their CI, through the Debricked web UI, or through any system the Customer has integrated using Debricked's APIs or Webhooks. Debricked also provides remediation advice and, for a subset of supported languages, automatic fixes of vulnerabilities.

SaaS Delivery Components

A detailed table and comparison can always be found at the bottom of this page: <https://debricked.com/pricing/>

SaaS Delivery Components			
Feature	Free	Premium	Enterprise
Vulnerability Management	Y	Y	Y
License Management	Y	Y	Y
License Reference	N	N	Y
Copyright Statement	N	N	Y
License Text	N	N	Y
Project Health (Open Source Select & Dependency Health Metrics)	Y	Y	Y
Policy Automations	Y	Y	Y
Start Left Policies	N	N	Y
Vulnerability Report	N	Y	Y
License Report	N	Y	Y
SBOM Report	N	N	Y

Unlimited Scans	N	Y	Y
Increased Compute	N	N	Y

SaaS Operational Services

SaaS Operational Services			
Feature	Free	Premium	Enterprise
SSO	N	N	Y
Chat & Email Support	Y	Y	Y
Dedicated CSM			Optional

Architecture Components

Debricked SaaS tool is a web-based user interface that provides SBOM creation, vulnerability scanning, license compliance scanning and community health scanning of all third-party components present in the Customers dependency/manifest files.

The tool can be used directly from a published CLI that can be run locally without the need to access the web-based user interface. Debricked also provides an API to access most functionality. In this case, the Debricked services can be used programmatically and be integrated with other tools.

Integrations

All supported CLI integrations are available to all tiers. See <https://portal.debricked.com/> for the list of supported SSO providers.

Languages supported

All supported languages are available to all tiers. See <https://portal.debricked.com/> for the list of supported languages.

Support Channels

The primary channel for support is the “Self-Serve” channel, which includes extensive public documentation, community, videos, and resources available at:

<https://portal.debricked.com/>

<https://debricked.com/blog/>

The Customer may contact Debricked through the support@debricked.com. The Debricked Support Team will either, at Micro Focus’s option, provide support to the Customer directly or coordinate delivery of this support. The severity of the request determines the response from the team.

Support Availability

Support is currently available in GMT+2 (Stockholm, Berlin, Copenhagen, Barcelona, Summertime) 09.00 to 17.00, not including national holidays.

Service Levels Based on Subscription Tier

Tier	Support Channels	Priority
Freemium	Self-Serve, Chat, Email	Micro Focus will make commercially reasonable efforts to respond to requests submitted by Freemium users.
Premium	Self-Serve, Chat, Email, Meeting/call	Every paying Customer will receive support in a timely manner.
Enterprise	Self-Serve, Chat, Email, Meeting/call, CSM On Request	Every paying Customer will receive support in a timely manner.

Service Monitoring and Performance Management

The Debricked tool is continuously monitored for performance issues and bugs. Proactive capacity and performance management procedures are in place so that the architecture of the environment meets the needs of its Customers.

This includes, but is not limited to:

- Monitoring uptime on all critical services
- Monitoring scan performance in real time
- Monitoring bugs by use of error logging tooling
- High test coverage on code to prevent new releases from introducing performance issues

Data Backup and Retention

The data backup and retention described in this section are part of Debricked'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:

- Repositories and commit IDs.
- Open-source dependencies. This is a list of dependencies and versions that have been identified by scanning a lock file, or if a lock file does not exist, by generating a dependency list from a provided dependency file.
- Tool configurations, such as events to trigger certain actions in the pipeline.
- Vulnerability status. This is a list of vulnerabilities that have been matched with the dependencies, together with user decisions for each vulnerability.
- Account users. This is the list of users that are associated with a given company account.

- License information and use cases. This is the licenses that are used for the respective packages together with a risk level for each license based on a user provided use case for the repository software.

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

Disaster Recovery for SaaS

Business Continuity Plan

Debricked continuously evaluates different risks that might affect the integrity and availability of SaaS. As part of this continuous evaluation, Debricked aligns with the Micro Focus developed policies, standards and processes that are implemented to reduce the probability of a continuous service disruption. Debricked documents its processes in a business continuity plan ("BCP") which includes a disaster recovery plan ("DRP"). Debricked 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.

The Debricked service is implemented over GCP technology service stack in one Availability Zone (AZ). The resources within a zone are distributed across multiple physical locations. This reduces the risk of a single point of failure since an outage in one location will be compensated by the other physical locations. The database instances are running in two different availability zones. This provides additional redundancy for the database instances.

Backups

Debricked performs both on-site and off-site backups with a 24 hours recovery point objective (RPO). Backup cycle occurs daily where a full copy of production data is replicated on GCP by our third-party database service provider. Backups are retained for the most recent seven (7) days. In addition, a continuously recorded binary log is kept such that we can retrieve data that is newer than what is in the latest full backup.

SaaS Security

Debricked takes measures to protect the confidentiality, availability and integrity of Customer Personal Data and confidential information.

Technical and Organizational Measures

Debricked 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 Debricked but represent a minimum standard. Customer remains responsible for determining the sufficiency of these measures.

Physical Access Controls

Debricked maintains physical security standards designed to prohibit unauthorized physical access to the Debricked equipment and facilities. All servers are stored offsite, either on GCP or at a secure location operated by a dedicated third-party. The Debricked facilities are monitored by video cameras and employees are issued access tags to enter the facilities.

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
- SaaS data is accessible only by authorized Debricked 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"
- Use of multi-factor authentication to provide state-of-the-art access to the SaaS systems

Availability Controls

Debricked continuously monitors the uptime of the service and takes immediate action to investigate and remedy any downtime. The monitoring of systems is designed to generate automatic alerts that notify Debricked of events such as a server crash, disconnected network, or delayed service for Customers. Debricked's business continuity management process includes a rehearsed method of restoring the ability to supply critical services upon a service disruption.

Data Segregation

Debricked scans Customer code and dependency files in separate pods. All pods are restored between scans so that no Customer data can leak between Customers. For CI/CD integrations, Debricked also provides the code to identify dependency files as open-source in order for Customers so that no source code is shared with Debricked.

Data Encryption

Debricked uses industry standard techniques to encrypt all 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. Debricked is included in this audit. A summary report or similar documentation will be provided to Customer upon request. Subject to Customer's execution of Debricked's standard confidentiality agreement, Debricked 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 Debricked confidential information.

In addition, Debricked runs and monitors a vulnerability disclosure program to allow independent researchers to submit any security issues through a responsible disclosure process.

Micro Focus Security Policies

Debricked 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”. Debricked regularly re-evaluates and updates its information and physical security program as the industry evolves, new technologies emerge, or new threats are identified.

Security Incident Response

In the event Debricked confirms a security incident resulted in the loss, unauthorized disclosure, or alteration of SaaS Data (“Security Incident”), Debricked will notify Customer of the Security Incident and work to reasonably mitigate the impact of such Security Incident. Should Customer believe that there has been unauthorized use of Customer’s account, credentials, or passwords, Customer must immediately notify Micro Focus Security Operations Center via softwaresoc@microfocus.com.

Micro Focus Employees and Subcontractors

Micro Focus requires that all employees involved in the processing of SaaS Data are authorized personnel with a need to access the SaaS Data, are bound by appropriate confidentiality obligations and have undergone appropriate training in the protection of Customer data. Micro Focus requires that any affiliate or third-party subcontractor involved in processing SaaS Data enters into a written agreement with Micro Focus, which includes confidentiality obligations substantially similar to those contained herein and appropriate to the nature of the processing involved.

Data Subject Requests

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

Service Decommissioning

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

Service Level Objectives

Debricked provides the following Service Level Commitments for the purpose of further measuring the quality of service that Debricked is delivering to the Customer.

Solution Provisioning Time SLO

Solution Provisioning is defined as the Debricked SCA SaaS solution being available for access over the internet. Micro Focus targets to make Debricked SCA SaaS available within five (5) business days of the Customer’s Order being booked within the Micro Focus order management system.

Solution Availability SLO

Solution Availability is defined as the Debricked SCA SaaS production application being available for access and use by Customer and its Authorized Users over the Internet. Debricked will provide Customer access to the

Debricked SCA SaaS production application on a twenty-four hour, seven days a week (24x7) basis at a rate of 99% ("Solution Uptime").

Measurement Method

On a monthly basis, the availability of the Debricked SCA SaaS Customer instance will be measured using the measurable days in the month (total days minus planned downtime, including maintenance, upgrades, etc.) as the denominator. The numerator is the denominator minus the number of days where a Customer account deadline is not met, to give the percentage of days that met the SLO (e.g., 30 days / 31 possible days = 96% availability). All SaaS monitoring will be paused at the beginning of each scheduled maintenance window and restarted at the completion of the window.

Boundaries and Exclusions

Performance and Availability SLO Metrics shall not apply in any of the following exceptions, and neither the Debricked SCA SaaS will be considered unavailable, nor any Service Level Failure be deemed to occur in connection with any failure to meet the requirement or impaired ability of Customer or its Authorized Users to access or use the Debricked SCA SaaS solution:

- 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 Debricked) or third parties beyond the control of Debricked
- Unavailability due to Customer equipment or third-party computer hardware, software, or network infrastructure not within the sole control of Debricked
- Scheduled maintenance
- Scheduled SaaS Upgrades

Initial SaaS Response Time SLO

The Initial SaaS Response Time refers to the support described herein. It is defined as the acknowledgment of the receipt of Customer’s request and the assignment of a case number for tracking purposes. Initial SaaS Response will come as an email to the requester and include the case number and links to track it using Micro Focus online customer portal. The Initial SaaS Response Time covers both service request and support requests. Micro Focus targets to provide the Initial SaaS Response no more than one hour after the successful submission of Customer’s request.

Incident Resolution

Based on support availability hours for Debricked Enterprise tier.

Severity Level	Technical response	Update Frequency	Target For Resolution	What Qualifies?
1	Immediate	Hourly	4 hours	Total or substantial failure of service. Known or suspected security events.
2	4 hours	Every 2 hours	8 hours	Unexpected significant degradation of service, major feature inability
3	4 hours	As available	Days, Depending on Customer impact or LOE	Performance issues outside the of the norm but not substantial enough to prevent usability of a feature.

4	As available	As available	Determined by the Customer impact or LOE	Bugs in deployed products not substantial enough to prevent required Customer functionality from being accessible but requiring development time to resolve.
---	--------------	--------------	--	--

Termination Data Retrieval Period SLO

When an account is terminated with Debricked all the data is immediately deleted. If the Customer wants a copy of the data, it must be requested ahead of time before termination.

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 the Debricked SaaS solution and associated components Manages contract issues
Security Lead	<ul style="list-style-type: none"> Leverages and educates other users about the product functionality designed by the Debricked SaaS solution Provides periodic feedback to the Debricked SaaS

Micro Focus Roles and Responsibilities

Micro Focus Role	Responsibilities
Customer Success Manager	<ul style="list-style-type: none"> Oversees the Customer onboarding and coaching best practices Serves as the Customer liaison to Micro Focus to ensure product adoption and engagement Coordinates Micro Focus resources internal
Technical Support Engineer	<ul style="list-style-type: none"> Primary point of contact for support queries
Account Manager / Sales Personnel	<ul style="list-style-type: none"> Manages the commercial relationship between the Customer and Micro Focus.

Assumptions and Dependencies

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

- Customer must have internet connectivity to access SaaS
- SaaS will be delivered remotely in English only
- A SaaS Order Term is valid for a single application deployment, which cannot be changed during the SaaS Order Term
- The service commencement date is the date on which Customer's Order is booked within the Micro Focus order management system
- The import of Customer data into SaaS during the implementation requires that the information is made available to Micro Focus at the appropriate step of the solution implementation and in the Micro Focus designated format
- Customer must ensure that its administrators maintain accurate contact information with Micro Focus
- Customer has determined, selected, and will use options in the Customer environment that are appropriate to meet its requirements, including information security controls, connectivity options, and business continuity, backup, and archival options
- Customer will establish and follow secure practices for individual account-based access for accountability and traceability

Furthermore, SaaS is provided based on the assumption that Customer will implement and maintain the following controls in its use of SaaS:

- Configuring Customer's browser and other clients to interact with SaaS
- Configuring Customer's network devices to access SaaS
- Appointing authorized users
- Configuring its SaaS account to require that end user passwords are sufficiently strong and properly managed
- Procedures for access approvals, modifications, and terminations.

Good Faith Cooperation

Customer acknowledges that Debricked'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 Debricked. 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 Debricked in performing its obligations under this Service Description, Debricked will not be liable for such failure or delay.