Heimdal®

Heimdal Security
General and Support Team

Service Level Agreement

1. Scope

1. This Service Level Agreement set out below (hereinafter referred to as "SLA") shall apply to all license agreements between Heimdal and Customers.

2. This document describes the standard level of service rendered by Heimdal for Customers, whether the purchase of the license has been made directly or via a Heimdal Partner, who have purchased its Product Services (PS), including availability of services, response times in case of product and/or service failure.

3. This service level agreement excludes coverage for the Managed Extended Detection and Response (referred to as "MXDR") product. To see coverage for the MXDR SLA, please consult the corresponding service agreement.

4. Heimdal reserves the right to change, update, amend and modify this SLA at any time. Such changes will be transmitted to the Customer in writing electronically within 30 days of the changes.

2. PS Service levels

1. The PS service shall generally perform to the levels as set forth below:

   a. Heimdal's software management and protection infrastructure must have a guaranteed up-time of minimum 99,9% at all times.

   b. Heimdal backend and management portal services must have a guaranteed up-time of minimum 99,5%.

   c. Heimdal's patch management coverage at 24/7/365 with 8-hour SLA and 4-hour deployment median.

2. The uptime of the service is expressed as a percentage of uptime in a given 12-month period. Heimdal provides the PS Service level in connection with the cloud services. Uptime and availability for the Heimdal Service are subject to and controlled by the cloud provider Service Level Agreement.

3. The uptime of the PS Service level for a given month will be calculated as follows (rounded to the nearest one-tenth of one percent): Availability % = 100% x (Total Minutes in the Month – Total Minutes Unavailable in the Month) / Total Minutes in the Month. The PS Services level will not be deemed unavailable for any downtime or outages relating to: (i) a Customer Outage Event, (ii) equipment, applications, interfaces, integrations, or systems not owned by Heimdal, or service not offered by Heimdal or (iii) a Force Majeure Event. "Customer Outage Event" means a period of time in which the Services are not available due to acts, omissions or requests of Customer, including without limitation (a) configuration changes in, or failures of, the Customer end of the network connection, (b) work performed by Heimdal at Customer's request, (c) Customer's unavailability or untimely response to incidents that require its participation for source identification and/or resolution or (d) Customer's failure to provide Heimdal with any requested physical or remote access to any Customer facilities, equipment or personnel emergency.

4. If the service deviates from the above SLA the Customer is entitled to an extension of the service, which is in direct proportion to the SLA deficiency.

5. If the SLA deficiency is greater than 10% of the SLA, the customer is entitled to a proportionate refund or cancellation.

3. Communication

1. Customers can communicate on topics such as technical issues, questions, feedback, bug reports, warranty claims with Heimdal's Support Team via E-mail to corpsupport@heimdalsecurity.com or telephone during working days to:

Phone:

UK +44 1445 700309
US +1 (855) 220-2405
DK +45 78 75 03 37

E-mailing and calling hours:

Mondays - Sunday 24/7/365

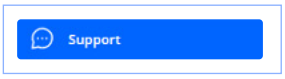
2. However, in order to receive the best response time and resolution we recommend the Customer to reach out to Heimdal's Technical Support Department by submitting a request via the Submit a request form. Submitting a request can be achieved in three ways:

- By visiting our website directly https://heimdalsecurity.com, clicking on the Support button, then on the Submit a request button, which will open the form to complete the details required.

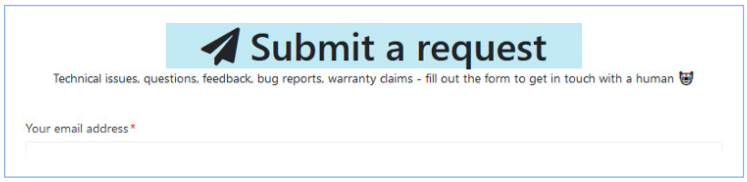
- By entering in your Browser, the following form link https://support.heimdalsecurity.com/hc/en-us/requests/new (fig 1)

- From the Heimdal Dashboard (login required), clicking on the button, then on the Submit a request button, which will open the form to complete the details required.

(fig 1)



(fig 2)



4. Heimdal Support Team response time

1. Heimdal's Support Team will respond to all submitted Customer requests according to the below classification outlined in the table.

Risk Rating	Description	Response time
Critical	Critical/Major Product and Service failure with complete interruption.	98% of all reported incidents will be responded to within 1 hour
High	Substantial Product and Service failures severely interrupting the Service or leading to major delays.	95% of all reported incidents will be responded within 4 hours
Medium	Standard Product and Service issues with no or negligible influence overall.	95% of all Service failures will be responded within 0-8 hours
Low	Requests for information with reference to Products and Services.	95% of all reported incidents will be responded between 0-8 hours

2. If an MXDR Customer opens a support case with Heimdal Support Team that case will fall under the General and Support Team SLA and not under the MXDR SLA. A support case is considered to be a case in which the problem is related to a Heimdal product, a problem caused by any of Heimdal product or a conflict between Heimdal product and a third-party vendor.

3. If an MXDR customer opens an incident case with our Support Team that case will fall under the MXDR SLA. An incident case is considered to be a case in which the problem is related to a malicious activity. A malicious activity can be described as an external threat that can harm or compromise an environment protected by Heimdal.

5. The average time from service degradation until rehabilitation

Risk Rating	Server-side (dashboard, DNS resolvers, core services, etc.)	Customer-side (agent related)
Critical	~1 hour	~24 hours
High	~4 hours	~48 hours
Medium	1 ~ 4 weeks (next scheduled release)	1 ~ 4 weeks (next scheduled release)

6.The average remediation time for conducted Penetration Testing

Risk Rating	Heimdal remediation commitment
Critical	Maximum 60 days from the date the testing report was issued, but sooner if technically possible, which typically also means a separate release cycle
High	Without any undue delay, still typically within a separate release cycle
Medium	At the first possible suitable option, as part of the normal release cycles
Low	At Heimdal's best convenience, as part of normal release cycles
Informational	If Heimdal considered that should be addressed

7. Patch Management

1. Heimdal is using a patch management process to ensure the security and performance of the products. As part of the patch management process, Heimdal ensures that:

a. All patches are tested on all the Operating Systems supported by the vendor before being deployed in production.

b. All patches are run in a sandbox environment and tested against malicious behavior with our Heimdal solution before being deployed in production.

c. All 3rd party tools and advertisement packages are removed from patches before being deployed in production.

8. Exclusions

1. This SLA does not apply in the following cases:

a. Scheduled maintenance (Customers are notified, ahead of time, through a Release Note via e-mail containing information such as the date, time and duration of the scheduled maintenance).

b. The failure is related to services which are not functions of Heimdal's PS.

c. The failure is caused by deliberate actions or omissions of the Customer or third parties.

d. Incident Response (addressing and managing the aftermath of a breach or cyber-attack, i.e., Ransomware attack), including but not limited to Initial Assessment, Investigation & Mitigation, Preservation of the Records, determining Legal and Notification Obligations.