Heimdal®

Privacy Data Sheet for Heimdal
Remote Desktop

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the Heimdal Remote Desktop Control product. This document provides detailed information about the types of data collected, how and where it is processed, and the measures in place to ensure compliance with global privacy regulations. It serves as a resource for customers to understand the data handling practices of Heimdal Security, ensuring transparency and trust in our commitment to safeguarding user data.

1. Product Summary

Heimdal Remote Desktop is a powerful solution designed to facilitate secure remote access to organizational systems. The product monitors and controls remote desktop sessions, enabling administrators to securely manage and oversee access to critical systems. With robust security measures, including session monitoring and the option for session recording, Heimdal Remote Desktop provides comprehensive protection for remote operations, ensuring that all activities are compliant with security and privacy standards.

2. Heimdal Remote Desktop Control – data processing

a. Remote Desktop Control – data processed

Type of data	Example(s)	Purpose of processing
Hostname	CUSTOMER-PC	To identify the endpoint
Username	User1	To identify specific user;
From – To hostname and username	CUSTOMER-PC; User1	To track remote sessions, the user that initiated the remote session and the recipient hostname and user
IP address	172.17.142.78	Used to initiate remote sessions
Version	4.4.0 RC	To track agent version
Last Seen	2024/09/16 17:56:18	Last time computer was seen online by the Heimdal server; used to know if a remote session can be initiated or not
Session Duration	Session length	Used for tracking and reporting

Type of data	Example(s)	Purpose of processing
Session Type	2024/09/16 17:56:18	Session start time, used for tracking and reporting
Session recording file name		Used for tracking and reporting
Timestamp		User to download the remote session recording
File password	2024/09/16 17:56:18	Recording creation date and time, used to track session recordings
Timestamp		Used to access the recording file

b. Remote Desktop Control – data flow

Heimdal Remote Desktop processes various types of data to facilitate secure remote access to organizational systems and to monitor and record sessions where necessary. The following outlines the specific data types processed and the methods involved:

- **Username Data:** The system processes usernames associated with each remote desktop session. This data is essential for authenticating users and ensuring that only authorized personnel have access to remote desktop services. It also helps in associating specific actions within a session to the corresponding user.

- **IP Address Data:** The IP addresses of both the user and the remote system are processed to establish and maintain secure connections. This data is used to track the origin and destination of the remote desktop session, providing an additional layer of security by verifying that connections are being made from trusted locations.

- **Session Recordings:** If session recording is enabled, the system captures and stores video recordings of the remote desktop sessions. These recordings are processed and stored securely to allow for auditing, training, and compliance purposes. The data captured includes everything that occurs on the screen during the session, including user actions, accessed files, and system interactions. Session recordings are securely stored by Heimdal.

All personal data processed by Heimdal Remote Desktop Control is handled in compliance with applicable privacy laws, including the General Data Protection Regulation (GDPR). Data is retained only for as long as necessary to fulfill its intended purpose and is protected by robust encryption and strict access controls to ensure the security and confidentiality of sensitive information.

This data processing is critical to providing secure remote desktop access, enabling comprehensive monitoring, and ensuring compliance with organizational and regulatory standards.

3. Processing Locations

For our Remote Desktop, we offer the following data storage options on Microsoft Azure, allowing customers to choose the location that best suits their regulatory and operational needs:

- **Azure Europe (Netherlands/Amsterdam):** This location is ideal for customers within the European Union who require compliance with GDPR and prefer to maintain their data within the European Economic Area.

By choosing this option, customers can ensure their data is stored in accordance with strict EU data protection laws, meeting all necessary data sovereignty requirements.

- **Azure UK (UK/London):** This option offers a dedicated solution for UK-based customers, ensuring that data is stored within the UK. This ensures compliance with local data protection regulations, particularly post-Brexit, and guarantees that data sovereignty is maintained according to UK-specific legal standards.

- **Azure US (US/Virginia):** This storage option is tailored for customers in the United States, providing a solution that aligns with U.S. compliance requirements, including those under HIPAA and other federal and state-specific regulations. Additionally, it ensures optimal data access speeds and performance for users within the North American region.

If a customer does not specify a preference, by default, data is stored within the European Union, thereby aligning with stringent EU data protection standards.

4. Compliance with Privacy Regulations

Heimdal Security is deeply committed to maintaining compliance with global privacy regulations and upholding the highest standards of data protection. Our solutions are designed and operated in compliance with several key privacy laws and standards, including:

- **GDPR (General Data Protection Regulation):** Heimdal Security adheres to all GDPR requirements, ensuring that personal data is processed lawfully, fairly, and transparently. We have implemented robust measures to protect the privacy rights of individuals within the European Union.

- **UK Data Protection Act 2018:** In the UK, we comply with the Data Protection Act, which complements the GDPR post-Brexit and includes provisions specific to the UK.

- **US Privacy Regulations:** Heimdal Security complies with relevant US privacy laws, including the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data protection and other state-specific regulations as applicable.

- **NIS2 Directive:** We align with the Network and Information Security (NIS2) Directive, which sets out the legal measures to boost the overall level of cybersecurity in the EU, particularly concerning critical infrastructure and essential services.

- **ISAE 3000 SOC 2 Certification:** Heimdal Security is certified under ISAE 3000 SOC 2, a widely recognized standard for managing customer data based on five trust service principles: security, availability, processing integrity, confidentiality, and privacy. This certification underscores our commitment to maintaining a secure environment for our customers' data.

5. Storage Period

For the Remote Desktop data is retained for a period of **2 years**. This duration is necessary to ensure effective threat detection and response, as well as to comply with relevant legal and regulatory requirements. After this period, the data is securely deleted from our systems unless longer retention is required by law or necessary for legitimate business purposes.