Privacy Data Sheet for Heimdal

Privileged Account and Session Management (PASM)

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the Heimdal Privileged Account and Session Management (PASM) solution. 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 data privacy.

1. Product Summary

Heimdal Privileged Account and Session Management (PASM) is a comprehensive security solution designed to manage, monitor, and control privileged accounts and their sessions within an organization. PASM helps to minimize the risks associated with the misuse of privileged accounts by providing centralized management, session recording, and real-time monitoring of privileged activities. The solution ensures that all actions performed by privileged users are logged, monitored, and auditable, significantly enhancing security and compliance efforts within the organization.

2. Privileged Account and Session Management (PASM) - data processing

a. Privileged Account and Session Management – data processed

Type of data	Example(s)	Purpose of processing
Server name	PASM-Server	Used from identifying unique PASM servers
No. of administrator accounts	2	User for licensing and reporting purposes
No. of user accounts	4	User for licensing and reporting purposes
Sessions completed	5	Used for reporting and tracking purposes
Sessions opened	5	Used for reporting and tracking purposes
Average session length	5	Used for reporting and tracking purposes

Type of data	Example(s)	Purpose of processing
Sessions recorded	5	Used for reporting and tracking purposes
Version	1.0.0.100	To track the specific version of the product
Last seen timestamp	2024/09/17 04:14:44	Displays the last time the server was seen online by the Heimdal servers and licensing was checked successfully

b. Privileged Account and Session Management – data flow

Heimdal Privileged Account and Session Management (PASM) processes various types of data to effectively manage privileged accounts and monitor their associated sessions. The data processing activities are designed to comply with relevant privacy regulations while maintaining a high standard of security and accountability. The types of data processed include:

- **Server Name:** The solution processes the server names chosen by the data controller to manage and monitor privileged sessions. This information is critical for organizing and associating sessions with the correct servers, enabling precise tracking and management of privileged activities.
- **Account Data:** The number of accounts, including both administrator and non-administrator users, is collected and processed. This data is used to monitor account usage, enforce access control policies, and ensure that only authorized users have access to privileged accounts. Tracking the number of accounts helps in managing user privileges and ensuring that least privilege principles are applied across the organization.
- **Usage Data:** The solution collects detailed usage data, including the number and length of sessions conducted by privileged users. This data is essential for monitoring the use of privileged accounts, detecting anomalies, and ensuring that all sessions are properly recorded and audited. The length of sessions and frequency of access are tracked to identify potential misuse or security risks associated with prolonged or excessive use of privileged accounts.
- **Session Recording Data:** Heimdal PASM records the activities performed during privileged sessions, including commands executed, files accessed, and configurations changed. This data is crucial for auditing purposes, allowing administrators to review session activities and ensure compliance with security policies. The recorded data provides a detailed audit trail that can be used to investigate security incidents or unauthorized actions.
- **Access Control Data:** The solution processes data related to access control mechanisms, including who accessed specific privileged accounts, when, and for what purpose. This data helps enforce strict access policies and ensures that privileged accounts are used only in accordance with organizational security standards.
- **Activity Logging Data:** All activities related to privileged account management and session monitoring are comprehensively logged. This includes user actions, accessed resources, and changes to system configurations. The activity logs are vital for maintaining accountability and for investigating any security incidents that may arise. The logs are securely stored and can be reviewed by administrators to ensure compliance with security policies and regulations.

Heimdal Privileged Account and Session Management (PASM) is engineered to process this data efficiently and securely, providing IT administrators with the tools they need to enforce strict control over privileged accounts and maintain a secure IT environment. The solution ensures that all data is processed in compliance with applicable privacy laws and handled with the utmost care to protect the privacy and security of users and their data.

3. Processing Locations

For our Privileged Account and Session Management (PASM), 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 Privileged Account and Session Management (PASM) 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.