Privacy Data Sheet for Heimdal

Privilege Elevation and Delegation Management (PEDM)

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the Heimdal Privilege Elevation and Delegation Management (PEDM) 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 Privilege Elevation and Delegation Management (PEDM) is a robust security solution designed to manage and control user privileges across an organization's endpoints. By providing granular control over user permissions, the PEDM solution minimizes the risk of unauthorized access and reduces the attack surface associated with elevated privileges. The solution allows organizations to elevate user privileges dynamically based on specific needs while ensuring that these privileges are limited and time-bound, significantly enhancing overall security. Additionally, the solution includes comprehensive logging and monitoring capabilities to track user activity and ensure compliance with security policies.

2. Privilege Elevation and Delegation Management (PEDM) - data processing

a. Privilege Elevation and Delegation Management – data processed

Type of data	Example(s)	Purpose of processing
Hostname	CUSTOMER-PC	To identify the endpoint
Username	User1	To identify the user that requested the elevation
Timestamp	Date and time of the request	Used for tracking, lists the date and time when the request was sent/ started
File path	C:\Users\test\app.exe	To elevate specific files
Application name	compmgmt.msc	Application name of the file selected for elevation

Type of data	Example(s)	Purpose of processing
Executed processes	C:\Windows\system32\Background-TaskHost.exe	Used to track all the executed processes during an elevated session
Elevation duration	60 minutes	Time spent by a user in elevated mode
User type	Administrator	Data retrieved in order to handle privileged access request

b. Privilege Elevation and Delegation Management – data flow

Heimdal Privilege Elevation and Delegation Management (PEDM) processes various types of data to ensure effective management of user privileges and to enhance security across the organization. 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:

- **Hostname and Username Data:** The PEDM solution collects and processes the hostname of devices along with the associated username. This data is crucial for identifying which users are associated with specific devices and for managing their privilege levels. The collection of hostname and username data allows the system to track and log actions related to privilege elevation, ensuring that only authorized users are granted elevated access when necessary.

- **Personal Applications Executed:** The solution monitors and logs the execution of personal applications on the endpoint devices. This data is used to detect unauthorized or potentially risky software usage, ensuring that only approved applications are executed within the environment. By tracking which applications are run under elevated privileges, the solution helps prevent the execution of malicious or unapproved software, thereby reducing security risks.

- **Privilege Elevation Data:** Data related to privilege elevation requests, including the time, duration, and scope of elevated privileges, is collected and processed. This includes details on what specific privileges were granted, to whom, and under what circumstances. The data is essential for auditing and reviewing the use of elevated privileges within the organization, ensuring that privilege elevation is done appropriately and securely.

- **Delegation and Access Control Data:** The PEDM solution also processes data related to the delegation of privileges, including who delegated the access, to whom it was delegated, and the permissions granted. This data is used to enforce access control policies and ensure that delegation is consistent with organizational security standards. The logging of delegation actions provides a detailed audit trail that can be reviewed to identify any unauthorized or inappropriate access.

- **Activity Logging Data:** All activities related to privilege elevation and delegation are logged comprehensively, including user actions, accessed resources, and changes to system configurations. This data is vital for maintaining accountability and for investigating any security incidents that may arise. The logs are stored securely and can be reviewed by administrators to ensure compliance with security policies and regulations.

Heimdal Privilege Elevation and Delegation Management (PEDM) is engineered to process this data efficiently and securely, providing IT administrators with the tools they need to enforce strict privilege controls 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 Privilege Elevation and Delegation Management (PEDM), 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 Privilege Elevation and Delegation Management (PEDM)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.