Heimdal®

Privacy Data Sheet for Heimdal
Application Control

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the Heimdal Application Control 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 Application Control is a robust security solution designed to manage and control the execution of applications within an organization's IT environment. By providing granular control over which applications can be executed on endpoints, the solution helps to prevent unauthorized or potentially malicious software from running, thereby reducing the organization's attack surface. Heimdal Application Control allows administrators to define application whitelisting and blacklisting policies, ensuring that only trusted applications are permitted to execute. This proactive approach to application management significantly enhances the security posture of the organization.

2. Application Control – data processing

a. Application Control – data processed

Type of data	Example(s)	Purpose of processing
Server name	PASM-Server	Used from identifying unique PASM servers
Hostname	CUSTOMER-PC	To identify the endpoint
Username	User1	To identify specific user
Process name	wmiprvse.exe	To identify process
File path	C:\program files (x86)\microsoft\edge\ application\msedge.exe	To identify the specific location of the detected file or application; Used for allowlist/blocklist
Number of executions	10	

Type of data	Example(s)	Purpose of processing
Publisher	Microsoft	
Software name	Google Chrome	To identify the specific software; Used for allowlist/blocklist
Software version	1.123.10	
MD5	Unique identifier of file	To identify specific file; Used for allowlist/blocklist
Timestamp	2024/06/27 11:38:31	Detection timestamp
Status	Blocked	State of the process: Blocked by default, Allow by default, etc, used for tracking the state of the detected process
Elevation status	Yes/No	Was the application elevated/ auto-elevated; Used to monitor the execution of processes with admin rights

b. Application Control – data flow

Heimdal Privileged Access Management and Application Control processes various types of data to ensure secure and efficient management of privileges and applications within your IT environment. The types of data processed include:

- **User Privilege Data:** Information about user permissions, including details on temporary and elevated access rights, is processed to control and monitor access to critical systems.
- **Application Execution Data:** Logs of applications executed by users, including those allowed, blocked, or monitored in passive mode, are processed to enforce security policies and maintain a comprehensive audit trail.
- **Audit Logs:** Detailed logs of all user actions and system responses are retained for 90 days to support compliance and security investigations.
- **Threat Intelligence Data:** Indicators of compromise (IoCs) and other relevant threat information are processed to enhance the system's ability to detect and respond to potential security threats.
- **User Activity Data:** Logs related to user actions, including escalation requests and system access attempts, are processed to ensure compliance and prevent unauthorized access.

All personal data is processed in compliance with applicable privacy laws, ensuring the utmost care in protecting user privacy and security.

3. Processing Locations

For our Application Control, 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 Application Control data is retained for a period of **90 days**. 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.