Privacy Data Sheet for Heimdal
Ransomware Encryption Protection

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the Heimdal Ransomware Encryption Protection product. It 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. This document serves as a resource for customers to understand Heimdal Security's data handling practices, emphasizing our commitment to transparency, data privacy, and the protection of sensitive information against ransomware threats.

1. Product Summary

Heimdal Ransomware Encryption Protection is a specialized security solution designed to prevent ransomware attacks by monitoring and controlling the execution of applications and processes within an organization's IT infrastructure. The product tracks and analyzes various data points, including hostnames, associated usernames, and executed applications, to detect and block unauthorized encryption activities in real-time. With its advanced threat intelligence and comprehensive logging capabilities, Heimdal Ransomware Encryption Protection provides critical safeguards for digital assets, helping organizations prevent data breaches and maintain compliance with security standards.

2. Heimdal Ransomware Encryption Protection – data processing

a. Ransomware Encryption Protection – data processed

Type of data	Example(s)	Purpose of processing
Hostname	CUSTOMER-PC	To identify the endpoint
Username	User1	To identify specific user
File path	C:\program files (x86)\microsoft\edge\ application\msedge.exe	To identify the specific location of the detected file or application; Used for exclusions
Process name	MaverickRansomware	Name of the detected file; Used for exclusions
MD5	Unique file identifier	Used for exclusions

Type of data	Example(s)	Purpose of processing
Timestamp	2024/06/27 12:55:01	Detection timestamp, used for tracking
Owner	DESKTOP1 \ Test	Full device owner, used for tracking
PID	Process identifier (eg: 9136)	To track individual processes
Status	Detected, Blocked	To track the state of each detection
Email	user@heimdal.com	To track individual cloud detections
AD Group	DevUser	To track user membership to AD Group in case of cloud detections
No. of affected file	10	Total affected file
Session status	Revoked	To identify the state of the session in case of detections

b. Ransomware Encryption Protection – data flow

Heimdal Ransomware Encryption Protection processes various types of data to effectively safeguard your systems against ransomware threats. The following outlines the specific data types processed and the methods involved:

- **Hostname Data:** The system processes the hostname of each device within your network. This data is used to identify and monitor the specific machines that are being protected against ransomware attacks. By associating hostname data with specific threats, the system can provide targeted protection and log which devices have encountered suspicious activities.
- **Username Data:** The username associated with each hostname is processed to track user-specific actions and their interaction with potentially malicious activities. This data helps in correlating suspicious activities to specific users, enabling more precise threat identification and response.
- **Personal Applications Executed:** Heimdal Ransomware Encryption Protection monitors and logs the applications executed on each device. This data is crucial for detecting unauthorized or unusual application behavior that might indicate the presence of ransomware. The system analyzes these logs to identify and block ransomware encryption attempts in real time.
- **Application Execution Logs:** Detailed logs of all application executions, including timestamps and outcomes (allowed, blocked, or monitored), are processed to provide a comprehensive audit trail. These logs are crucial for post-incident analysis and compliance reporting, ensuring that any attempts at unauthorized encryption are fully documented.
- **Threat Intelligence Data:** The system continuously processes threat intelligence data, including indicators of compromise (IoCs) related to known ransomware strains. This data is used to update the protective measures and ensure the system is equipped to handle the latest ransomware threats.

All personal data processed by Heimdal Ransomware Encryption Protection is handled in compliance with applicable privacy laws, including the General Data Protection Regulation (GDPR). The data is processed to provide robust protection against ransomware while ensuring user privacy is respected. Data is retained for the duration necessary to fulfill its intended purpose and is secured through industry-standard encryption and access control measures.

This data processing is essential to maintain a secure environment, prevent ransomware attacks, and ensure the continued protection and compliance of your IT infrastructure.

3. Processing Locations

For our Ransomware Encryption Protection, 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 Ransomware Encryption Protection data is retained for a period of **90 days for endpoint; 2 years for cloud**. 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.