Privacy Data Sheet for Heimdal
Email Security

Introduction

This Privacy Data Sheet outlines the privacy practices associated with Heimdal Email Security. This document provides comprehensive 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 is intended to help customers understand the data handling practices of Heimdal Security, ensuring transparency and trust in our commitment to data privacy.

1. Product Summary

Heimdal Email Security is a robust security solution designed to protect organizations from email-based threats such as phishing, fraud, and malware. The product monitors and analyzes various components of email communications, including content, attachments, and metadata, to detect and prevent malicious activities. By leveraging advanced threat intelligence and real-time analysis, Heimdal Email Security provides essential safeguards that protect sensitive information and maintain the integrity of your organization's email systems.

2. Heimdal Email Security – data processing

a. Email Security - data processed

Type of data	Example(s)	Purpose of processing
FROM email address (sender)	sender@somedomain.com	Email processed as part of email send-receive flow
TO email address (recipient)	receiver@otherdomain.com	Email processed as part of email send-receive flow
Header From	bounces+814387-sender=somedo-main.com@otherdomain.com	Header processed as part of email send-receive flow
Timestamp	2024/09/19 18:03:39	Timestamp when email was processed (delivered, quarantined, etc), used for tracking
Subject	Based on provided items from the customer	Subject processed as part of email send-receive flow
TLS Received:	TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256 bits)	Addition security information
TLS Delivery:	TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256 bits)	Addition security information

Type of data	Example(s)	Purpose of processing
Source IP:	167.89.49.187	Addition security information
Destination IP:	167.89.49.187	Addition security information
Email header	X-Envelope-Recipient: receiver@oth-erdomain.com.....	Addition security information
Email body	Based on provided items from the customer	Subject processed as part of email send-receive flow; Used for flagging malicious content that may be included in email body
Size	175434 Bytes	Size processed as part of email send-receive flow;
Attachments	Based on provided items from the customer	Attachments processed as part of email send-receive flow; used for scanning malicious attachments

b. Email Security - data flow

Heimdal Email Security processes various types of data to detect and prevent fraudulent email activities. The following outlines the specific data types processed and the methods involved:

- **Email Content:** The system analyzes the content of emails, including text within the email body, to identify indicators of phishing, fraud, or other malicious activities. This analysis is essential for detecting and preventing email-based threats before they reach the intended recipient.
- **Email Attachments:** Attachments within emails are scanned and analyzed for malicious content, such as viruses, malware, or ransomware. The system examines file types, checks for known signatures, and may run attachments in a secure environment to detect hidden threats.
- **Email Subject:** The subject lines of emails are processed to identify suspicious or unusual patterns that may indicate phishing or social engineering attempts. This data is cross-referenced with known threat patterns to enhance detection accuracy.
- **Email Addresses:** Both the sender's and recipient's email addresses are processed to verify the legitimacy of the communication. The system checks against a database of known malicious or spoofed email addresses and flags any suspicious activity for further review.
- **Source & Destination IP Addresses:** The IP addresses associated with the email's origin and destination are analyzed to detect potential fraud. This includes checking for IP addresses known to be associated with spam or malicious activities and ensuring that emails are originating from expected and trusted locations.
- **Threat Intelligence Data:** The system continuously processes threat intelligence data, including known phishing domains, IP addresses, and email templates used in fraud attempts. This data enhances the system's ability to proactively block fraudulent emails.

3. Processing Locations

For our Heimdal Email Security, 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 Email Security, data retention periods can be set to **none, 30 days, 90 days, or 1 year**, depending on user preferences. These retention durations are essential for ensuring effective threat detection and response, as well as for meeting legal and regulatory obligations. After the specified retention period, the data is securely deleted from our systems unless a longer retention period is required by law or needed for legitimate business purposes.