Heimdal®

Privacy Data Sheet for Heimdal

DNS Security – Endpoint

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the **Heimdal DNS Security – Endpoint**. 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 DNS Security – Endpoint is a powerful endpoint security solution designed to prevent cyber threats such as malware, phishing, and data breaches by filtering DNS traffic directly on the endpoint device. The product works by redirecting DNS requests from the operating system to a local DNS server on the endpoint, where they are analyzed to determine whether they should be allowed or blocked. This solution provides robust, real-time protection at the endpoint level, ensuring that users can safely browse the internet and access network resources without falling victim to cyber attacks.

2. Heimdal DNS Security – Endpoint - data processing

a. DNS Security Endpoint – data processed

Type of data	Example(s)	Purpose of processing
IP Address	Customer-PC	Identifying the customer's endpoint that performed the DNS request
Domain name	example.com	To analyze the DNS request by the domain name and decide whether it is a known malicious domain or not
Timestamp	Date of the request	To identify when a potential threat happened
TTPC (threat-to-process-corellation)	The full path of the executable that made the DNS request , e.g. C:\Temp\Myprogram.exe	To identify whether an unwanted software performed a DNS request for a malicious domain
Resolved Ips	If the DNS request is of type A record, the Ips it resolves to	Additional metadata info for the resolved domain
Resolved domains	If the DNS request is of type CNAME, the domain names it resolves to	Additional metadata info for the resolved domain

Type of data	Example(s)	Purpose of processing
URLs	If the domain was requested due to an HTTP(s) request, the original URL that was requested is also being logged	Additional metadata info for the resolved domain

b. DNS Security Endpoint – data flow

Heimdal DNS Security – Endpoint processes various types of data to ensure effective threat prevention and to provide users with a secure experience. The types of data processed include:

- **Network Traffic Data:** This includes DNS request information such as domain names, hostnames, and corresponding IP addresses queried by users. This data is crucial for detecting and blocking malicious activities in real-time.
- **DNS for Endpoint Data:** For the DNS Security – Endpoint solution, the data processed includes the source and destination domain names of DNS requests. This data is analyzed locally on the endpoint using a local DNS server (with IP addresses in the range of 127.0.0.3 - 127.0.0.254) to determine whether the request should be allowed or blocked. Importantly, the analysis does not access or interpret the content of the data being transmitted, ensuring the privacy and security of sensitive information communicated during DNS queries.
- **Threat Intelligence Data:** Collected to enhance the solution's ability to identify and respond to threats, this data includes indicators of compromise (IoCs) such as known malicious domains, IP addresses, and other relevant threat information. This data is used to update and refine threat detection mechanisms in real-time.
- **User Data:** Limited user identifiers, including IP addresses and user activity logs related to security events, are processed to associate network traffic with specific users or devices. This enables more precise threat detection and response, enhancing the security of the overall network environment.
- **Anonymized Data:** Where possible, data is anonymized to protect user privacy while still allowing for the detection and analysis of threats. Anonymization ensures that personally identifiable information (PII) is not exposed during the data processing activities.

Heimdal DNS Security – Endpoint enhances security by redirecting all DNS traffic from the operating system to a local DNS server on the endpoint. This local server analyzes DNS requests strictly based on the source and destination domain name, without accessing or interpreting the content of the data being transmitted. This approach guarantees that sensitive data communicated during DNS queries is protected, maintaining the confidentiality and privacy of user interactions with the network.

All personal data is processed in compliance with applicable privacy laws and is handled with the utmost care to ensure the privacy and security of users.

3. Processing Locations and Data Storage

Customers at Heimdal have the privilege to select the location where their data is stored, depending on the product they use. This choice allows businesses to meet specific data residency requirements and helps in complying with regional data protection regulations. 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.

Heimdal utilizes Microsoft Azure for data storage, offering the following options to meet diverse geographical and regulatory 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.

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 DNS Security – Endpoint solution is 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. Privacy and Data Security

Heimdal DNS Security – Endpoint is engineered to protect endpoint devices while ensuring the privacy of sensitive data. The solution is designed to analyze DNS requests based solely on the source and destination domain names, **without accessing or interpreting web traffic content or local files on the endpoint.**

This ensures that sensitive data, such as PHI (Protected Health Information) and PII (Personally Identifiable Information), communicated during DNS queries or handled locally by users, remains secure and private.

6. Storage Period

For the DNS Security – Endpoint solution, 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.