Privacy Data Sheet for Heimdal

DNS Security - Network

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the **Heimdal DNS Security – Network**. 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 - Network is a comprehensive network security solution that utilizes DNS filtering to prevent cyber threats such as malware, phishing, and data breaches. The product monitors and filters DNS requests across an organization's network, blocking malicious domains and ensuring safe internet browsing. With real-time threat intelligence and proactive threat hunting capabilities, Heimdal Threat Prevention Network delivers robust protection that is essential for safeguarding your digital assets.

2. Heimdal DNS Security – Network - data processing

a. DNS Security Network – data processed

Type of data	Example(s)	Purpose of processing
IP Address	Public IP address of the customer for incoming requests	Identifying the customer by the IP address of incoming DNS requests
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	Only if the logagent is present, to identify the underlying hostname that performed the DNS request
Hostname	CUSTOMER-PC	Only if the logagent is present, to identify the underlying hostname that performed the DNS request
Private IP Address	192.168.0.34	Only if the logagent is present, the private IP address of the device performing the DNS request is being logged to allow a deeper identification of the threat.

b. DNS Security Network – data flow

Heimdal Threat Prevention Network 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 and corresponding IP addresses queried by users. This data is crucial for detecting and blocking malicious activities in real-time.
- **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.
- **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, enabling more precise threat detection and response.
- **Anonymized Data:** Where possible, data is anonymized to protect user privacy while still allowing for the detection and analysis of threats.

Heimdal DNS Security - Network enhances security by providing customers a cloud DNS resolver to be used as forwarder for the entire organization. Furthermore, the Heimdal LogAgent utility can be installed on the customer's DNS server to map the hostnames and private IPs of the underlying devices to the DNS requests performed against the Heimdal DNS Security – Network DNS servers.

All 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

For our DNS Security Network product, we offer the following data storage options on Amazon Web Services (AWS), allowing customers to choose the location that best suits their regulatory and operational needs:

- **AWS Europe (Germany/Frankfurt):** This location is ideal for customers who require data storage within the European Union to comply with GDPR and other European data protection laws. By selecting this option, customers can ensure that their data remains within EU borders, meeting strict data sovereignty requirements.
- **AWS UK (UK/London):** This option serves customers who prefer their data to be stored in the UK, particularly accommodating post-Brexit data sovereignty requirements. Data stored in this location complies with UK data protection laws, ensuring that customers' data is handled according to local regulations.
- **AWS US (US/Virginia):** Catering to customers in the United States, this option ensures compliance with US data protection regulations and provides fast, reliable service to North American users. This location is suitable for organizations that need to adhere to US data privacy laws and wish to ensure optimal performance for their operations in the 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 Network 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. Storage Period

For the DNS Security Network data is retained for a period of **30 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.