Privacy Data Sheet for Heimdal
Patch & Asset Management

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the Heimdal Patch & Asset Management 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 Patch & Asset Management is a comprehensive endpoint management solution that automates the deployment of software patches and updates across an organization's IT infrastructure. This product ensures that all software applications and operating systems are up-to-date, significantly reducing the risk of vulnerabilities that could be exploited by cyber threats. In addition to patch management, the solution provides detailed asset management capabilities, enabling IT administrators to maintain an accurate inventory of all software and hardware assets within the organization. By keeping systems secure and compliant, Heimdal Patch & Asset Management plays a crucial role in safeguarding your digital assets.

2. Patch and Asset Management – data processing

a. Patch and Asset Management – data processed

Type of data	Example(s)	Purpose of processing
IP Address	Customer-PC	To identify the endpoint on which the patch is installed
Domain name	User1	To identify the specific username
Software name	Google Chrome	To identify the installed software
Software version	1.0.2	To identify the software version
Timestamp	Date of the install/software detection	To identify the date when the software was installed or detected as installed by Heimdal
Application GUID	Globally unique identifier for software application/patch	To uniquely identify the software or patch

Type of data	Example(s)	Purpose of processing
Installed OS Updates	Feature update to Windows 10, version 22H2	To retrieve successfully installed OS updates through Heimdal for each endpoint
Pending OS Updates	Feature update to Windows 10, version 22H2	To retrieve pending OS processed through Heimda update for each endpoint
Available OS Updates	Feature update to Windows 10, version 22H2	To retrieve available OS updates for each endpoint

b.Patch and Asset Management – data flow

Heimdal Patch & Asset Management processes various types of data to ensure effective software patching and asset management while maintaining security and compliance across the organization. The types of data processed include:

- **System and Application Data:** The solution collects and processes data related to the software applications and operating systems installed on each endpoint. This includes the name of installed 3rd party applications, their versions, the name of available and installed operating system updates, version information, installation status, and patch levels. The collected data is used to identify systems that require updates and to automate the deployment of patches, ensuring that all endpoints remain secure against known vulnerabilities.

- **Device Identification Data:** Heimdal Patch & Asset Management gathers data such as device identifiers (e.g., hostname, MAC address, IP address) to accurately inventory and manage all assets within the organization. This data is essential for associating specific devices with their corresponding software and hardware configurations, enabling precise tracking and management.

- **Patch Deployment Data:** Information related to the deployment of patches, including success/failure status, deployment times, and user interaction data, is collected to monitor the effectiveness of the patch management process. This data helps administrators ensure that patches are applied successfully and in a timely manner across the entire organization.

- **Asset Inventory Data:** The solution maintains a detailed inventory of both hardware and software assets within the organization. This includes information on installed applications, software licenses, hardware components, and device configurations. The asset inventory data is crucial for maintaining compliance with licensing agreements and for supporting strategic IT planning and budgeting.

- **User Interaction Data:** Limited data on user interactions with the Patch & Asset Management system, such as user credentials (e.g., username associated with the hostname and device management tasks) and activity logs, is processed to track administrative actions and ensure accountability in the management of IT assets.

Heimdal Patch & Asset Management is engineered to process this data efficiently and securely, automating the patch management process and providing IT administrators with the tools they need to maintain a secure and compliant IT environment. The solution ensures that all data is processed in compliance with applicable privacy laws and handled with the utmost care to protect the privacy and security of users and their data.

3. Processing Locations

For our Heimdal Patch & Asset Management, 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. Privacy and Data Security

For the Heimdal Patch & Asset Management 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.