Heimdal®

Privacy Data Sheet for Heimdal

Next-Gen Anti-Virus, Firewall & MDM

Introduction

This Privacy Data Sheet outlines the privacy practices associated with the Heimdal Next-Gen Anti-Virus, Firewall & MDM 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 NGAV (Next-Generation Antivirus) + XTP (Extended Threat Protection) with MDM (Mobile Device Management) is a comprehensive endpoint security solution designed to protect against a wide range of cyber threats, including malware, ransomware, phishing, and advanced persistent threats (APTs). The product combines advanced antivirus capabilities with extended threat protection and mobile device management, offering robust defense mechanisms across all endpoints, including mobile devices. With real-time threat intelligence, proactive threat hunting, and centralized management, Heimdal NGAV + XTP & MDM ensures that your digital assets are safeguarded against both known and emerging threats.

2. Heimdal NGAV + XTP & MDM – data processing

a. NGAV + XTP & MDM – data processed

Type of data	Example(s)	Purpose of processing
Server name	CUSTOMER-PC	To identify the endpoint
Hostname	User1	To identify specific user
Username	C:\program files (x86)\microsoft\edge\ application\msedge.exe	To identify the specific location of the detected file or application; Used for exclusions
Timestamp	2024/06/29 13:39:49	To identify exact time of a detection/ FW rule application/scan
Rule details	Profile type, Protocol, etc	Additional details used when creating the FW rule: Port, Profile type, Protocol, Direction, Permission
Local IP	1.1.1.1	Used to track the local IP of the user

Type of data	Example(s)	Purpose of processing
Remote IPs	1.2.3.4	Used to track the remote IP that triggered an alerts
No. of attempts	10	Total number of attempts for each alert
Alert timestamp	2024/08/27 13:05:12	Detection time of the FW alert
Detection type	Brute Force Attack Private	To identify the type of detection
MD5	Unique identifier of file	To identify specific file
Filename	pe_lab_gen.exe	Name of the detected file;
Status/resolution	Infected	Used to track specific state of files- Removed, Infected, Quarantined

b. NGAV + XTP & MDM – data flow

Heimdal NGAV + XTP with MDM processes various types of data to ensure effective threat prevention and to provide users with a secure experience. The types of data processed include:

- **Hostname and Username Data:** The system collects and processes the hostname of the devices along with the associated username. This data is essential for linking security events to specific users and devices, allowing for more accurate threat detection and response.
- **Personal Applications Executed:** The solution monitors and logs the execution of personal applications on the endpoint devices. This data helps in detecting potentially malicious activities and ensuring that only approved software is running on the network, enhancing overall security.
- **Endpoint Security Data:** This includes information related to malware detection, file scanning results, and threat signatures. The data is crucial for identifying and mitigating potential security threats in real-time.
- **NGAV and Windows Defender Integration:** Our Next-Generation Antivirus (NGAV) solution leverages Windows Defender as a baseline to scan any files that are created or altered on the system, including files downloaded during web services interactions. This real-time scanning focuses on detecting malicious threats during file creation or modification events, without examining the contents of the files. Thus, while we ensure robust protection against malware, the privacy of your PHI (Protected Health Information) and PII (Personally Identifiable Information) data is maintained as the content of the files remains unexamined.
- **Network Traffic Data:** Collected as part of the extended threat protection features, this data includes IP addresses, domain names, and other network-related information that is analyzed to detect and block malicious activities. The focus is on the patterns of traffic rather than the content of the data being transmitted.
- **Mobile Device Management Data:** For MDM functionality, data such as device identifiers, security settings, and application usage is processed. This data helps administrators manage and secure mobile devices within the organization, ensuring compliance with security policies.

- **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. It is used to update and refine the detection capabilities of the system continuously.

- **User Data:** Limited user identifiers, including IP addresses and activity logs related to security events, are processed to associate security incidents with specific users or devices. This enables precise threat detection and response, enhancing the overall security posture of the organization.

- **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 NGAV + XTP with MDM enhances security by providing a centralized platform that integrates antivirus, threat protection, and mobile device management functionalities. The system focuses on analyzing security-related data while ensuring that the content of user communications and local files remains private. This approach guarantees that sensitive data handled by the solution is protected, maintaining the confidentiality and security of all user interactions with the network.

3. Processing Locations

For our Next-Gen Anti-Virus, Firewall & MDM, 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 Next-Gen Anti-Virus, Firewall & MDM 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.