Privacy Datasheet

Intro

NinjaRMM engaged independent data privacy risk management provider TrustArc™ to review and document the data flows and practices described in this datasheet. The purpose of this document is to provide customers of NinjaRMM with information needed to assess the impact of NinjaRMM's cloud-based Remote Monitoring and Management platform on their overall privacy posture by detailing how personal information may be captured, processed and stored by and within NinjaRMM and its associated products.

TrustArc
the new TRUSTe

Product Summary

NinjaRMM is the world's first security centric remote monitoring and management platform. NinjaRMM touts an amazing user experience, 360-degree monitoring, an IT marketplace and tight integrations with products used by MSPs as well as IT professionals. NinjaRMM is designed to work with small one-person shops to large enterprise service companies providing full SLA service offerings.

Type	Reason
Cookie and Usage Data	Analytics, Advertising, Remarketing and behavioral targeting
Company name, country, email address, first name, last name, number of employees, phone number, state, website and ZIP/Postal code	Provision of services, contacting a user Phone number
Phone number	Phone call
Payment information	Handling payments (through 3rd party Stripe)
Usage Data	Heat mapping and improvement of services
Social media information	Facebook Custom Audience and other social media services to inform customers about NinjaRMM news

Customer Privacy Options

NinjaRMM collects data that is necessary to fulfill its services regarding the obligations to its customers. Users can choose how they want to be contacted both for sales or service functions. As NinjaRMM provides an ecosystem of products, the customer has the choice which 3rd party services are used and to which 3rd party their data (to fulfill services) will be transmitted. All 3rd parties are GDPR compliant and have signed a Data Processing Agreement with NinjaRMM.

Customers can access their data through the NinjaRMM online platform and make adjustments to their data and how their data is being used.

Also, customers and users have the right to contact NinjaRMM, either via phone or email at privacy@ninjarmm.com, to have their data accessed, assessed, altered, corrected or deleted. Customers and users have all rights, as specified in Article 12-23 of the GDPR, i.e., the right to object in certain circumstances, the right to withdraw consent, the right to have the personal data collected provided to them or the right to not being subject to decision-based processing based solely on automated processes.

Access to Data

Physical security is maintained both at premises perimeter and at building entry points. Staff is required to use two-factor authentication multiple times to enter data center floors. 3rd party data storage providers are governed and controlled by contract and have signed a Data Processing Agreement. Virtual access for NinjaRMM employees is restricted to access that is needed to fulfill their function. Staff is trained in data security and GDPR requirements audited and trained on a regular basis.

Sales staff needs to have access to necessary customer information to fulfill orders or contractual obligations. Customer Service and Tech Support staff will have access to primary customer data to meet support requests and full access to a user account if granted by the user. Full access can, e.g., given via a remote support session and will only be valid and possible during a Tech Support session. Staff will no longer have full access will once a support session finishes or once the user revokes permission.

Retention

NinjaRMM will retain information for as long as an account is active. Once services have been discontinued, the user has the right to withdraw his consent and ask for erasure. After closing your account, NinjaRMM will keep information up to 3 months for an easy possibility to restart services. Storage beyond this limit is solely based on the necessity to comply with any applicable legal obligations.

Security

Data storage
Passwords are encrypted using industry-standard cryptographic algorithms and key lengths. All data is stored on secure, non-publicly-accessible servers and media. Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, and snapshots. Encrypted data use the industry standard AES-256 encryption algorithm to encrypt your data. This will fulfill compliance requirements for data-at-rest encryption. To manage the keys used for encrypting and decrypting use an enterprise-grade key management system scaled for the cloud. Will define compliance policies that control how these keys can be used with full auditing capability to verify that keys are being used appropriately. All logs, backups, and snapshots are encrypted as well.

Network Security
Ninja infrastructure runs within a virtual private cloud (VPC) at a highly secure data center with built-in network firewalls. All data is transmitted between the Ninja infrastructure, and 3rd-party endpoints are secured by TLS encryption. Legacy (insecure) SSL 2/3 protocols are disabled. All data transmitted from Ninja monitored endpoints to Ninja infrastructure is secured by TLS encryption. Legacy (insecure) SSL 2/3 protocols are disabled. Ninja staff access to customer data is tightly controlled. The Ninja platform provides multi-factor authentication to allow users to further secure access to their customers' operational data. Redundant diagnostic tools continually monitor the Ninja platform infrastructure. Staff is prepared to

respond to availability-impacting incidents 24x7x365. The Ninja platform allocates a tenanted database instance per customer to cleanly separate customer data.

Data Center Physical Security

Physical security is maintained both at premises perimeter and at building entry points. Staff is required to use two-factor authentication multiple times to enter data center floors. Data center supplied with fully-redundant power supply, including UPS systems and facility-wide generator support. The data center is fully climate-controlled, with automatic fire detection and suppression equipment installed. Data on decommissioned storage devices is destroyed using industry-standard best-practice methods.

On-going Network Security Maintenance & Audits

Security updates are regularly installed for operating systems, and for commercial and open source frameworks. Ninja IT administrative staff performs regular security audits. Security audits include (a) Review of administrator accounts, credentials, and access logs and (b) Automated analysis of server access logs.

External Links/Resources

For additional information, please visit the following documents:
Cookie policy https://ninjarmm.com/cookie-policy/
Privacy policy https://ninjarmm.com/privacy-policy/
GDPR policy https://ninjarmm.com/gdpr-policy/

About this Datasheet

The information contained herein is based upon document reviews and interviews with relevant subject matter experts involved in the development and operation of the services described. The discovery process relied upon the good faith accuracy of the information provided; TrustArc has not undertaken an independent audit and does not certify the information contained in this datasheet. However, the information contained herein was believed to be accurate and complete as of the time this datasheet was first published. Please note that the information provided with this paper, concerning technical or professional subject matters, is for general awareness only, may be subject to change and does not constitute legal or professional advice, nor warranty of fitness for a particular purpose or compliance with applicable laws.

For more information visit
www.ninjarmm.com