CloudNuro

We offer a comprehensive AI platform that manages cloud applications, subscriptions, renewals, consumptions, account management, budgeting, and integrations. We focus on AI-driven predictive analytics to forecast cloud consumptions and deploy on Google Cloud Platform with the highest level of security and maximum availability.

✉ Contact: info@cloudnuro.com

This Trust Report is powered by Vanta. Vanta identifies security flaws and privacy gaps in a company's security posture by connecting to core systems to continuously monitor an organization's cloud infrastructure, endpoints, corporate procedures, enterprise risk, and employee accounts.

Thousands of fast-growing companies trust Vanta to automate their security monitoring and compliance process.

Learn more

This Trust Packet was exported on Sun Sep 18 2022.

Monitoring

● Updated an hour ago

Infrastructure security

Service infrastructure maintained

The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. ✓

Production data backups conducted

The company performs periodic backups for production data. Data is backed up to a different location than the production system. ✓

Intrusion detection system utilized

The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches. ✓

Database replication utilized

The company's databases are replicated to a secondary data center in real-time. Alerts are configured to notify administrators if replication fails. ✓

Production database access restricted

The company restricts privileged access to databases to authorized users with a business need. ✓

Remote access MFA enforced

The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. ✓

Access revoked upon termination

The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. ✓

Production network access restricted

The company restricts privileged access to the production network to authorized users with a business need. ✓

Unique production database authentication enforced

The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key. ✓

Remote access encrypted enforced

The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. ✓

Encryption key access restricted

The company restricts privileged access to encryption keys to authorized users with a business need. ✓

Production data segmented

The company prohibits confidential or sensitive customer data, by policy, from being used or stored in non-production systems/environments. ✓

Access control procedures established

The company's access control policy documents the requirements for the following access control functions: adding new users, modifying users, and/or removing an existing user's access. ✓

Log management utilized

The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. ✓

Network segmentation implemented ✓

The company's network is segmented to prevent unauthorized access to customer data.

Unique network system authentication enforced ✓

The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.

Firewall access restricted ✓

The company restricts privileged access to the firewall to authorized users with a business need.

Organizational security

Portable media encrypted ✓

The company encrypts portable and removable media devices when used.

Anti-malware technology utilized ✓

The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

Employee background checks performed ✓

The company performs background checks on new employees.

MDM system utilized ✓

The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.

Password policy enforced ✓

The company requires passwords for in-scope system components to be configured according to the company's policy.

Security awareness training implemented ✓

The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.

Confidentiality Agreement acknowledged by contractors ✓

The company requires contractors to sign a confidentiality agreement at the time of engagement.

Production inventory maintained ✓

The company maintains a formal inventory of production system assets.

Confidentiality Agreement acknowledged by employees ✓

The company requires employees to sign a confidentiality agreement during onboarding.

Asset disposal procedures utilized ✓

The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.

Product security

Penetration testing performed ✓

The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.

This Trust Packet was exported on Sun Sep 18 2022.

Data encryption utilized

The company's datastores housing sensitive customer data are encrypted at rest. ✓

Data transmission encrypted

The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. ✓

System activity logged

The company captures system activity, including user activity, in transaction logs. ✓

Vulnerability and system monitoring procedures established

The company's formal policies outline the requirements for the following functions related to IT / Engineering: vulnerability management, system monitoring. ✓

Internal security procedures

Vulnerabilities scanned and remediated

Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. ✓

Access reviews conducted

The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. ✓

Continuity and disaster recovery plans tested

The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually. ✓

Incident response plan tested

The company tests their incident response plan at least annually. ✓

Access requests required

The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. ✓

Backup processes established

The company's data backup policy documents requirements for backup and recovery of customer data. ✓

Production deployment access restricted

The company restricts access to migrate changes to production to authorized personnel. ✓

Vendor management program established

The company has a vendor management program in place. Components of this program include: critical third-party vendor inventory, vendor's security and privacy requirements, and review of critical third-party vendors at least annually. ✓

Incident response policies established

The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. ✓

Change management procedures enforced

The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. ✓

This Trust Packet was exported on Sun Sep 18 2022.

Configuration management system established

The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment. ✓

Management roles and responsibilities defined

The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. ✓

Service description communicated

The company provides a description of its products and services to internal and external users. ✓

Security policies established and reviewed

The company's information security policies and procedures are documented and reviewed at least annually. ✓

Support system available

The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. ✓

Roles and responsibilities specified

Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. ✓

Data center access reviewed

The company reviews access to the data centers at least annually. ✓

Physical access processes established

The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners. ✓

Third-party agreements established

The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity. ✓

Incident management procedures followed

The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. ✓

Development lifecycle established

The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements. ✓

Continuity and Disaster Recovery plans established

The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. ✓

Data and privacy

Privacy policy established

The company has a privacy policy is in place that documents and clearly communicates to individuals the extent of personal information collected, the company's obligations, the individual's rights to access, update, or erase their personal information, and an up-to-date point of contact where ✓

Customer data deleted upon leave

The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service. ✓

Data retention procedures established

The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. ✓

Privacy compliant procedures established

The company has documented processes and procedures in place to ensure that any privacy-related complaints are addressed, and the resolution is documented in the company's designated tracking system and communicated to the individual. ✓

Customer data retained

The company retains customer transaction data for the life of a customer account. No historic transaction data is purged until the customer account is deleted. ✓

Privacy policy available

The company has a privacy policy available to customers, employees, and/or relevant third parties who need them before and/or at the time information is collected from the individual. ✓

Privacy policy reviewed

The company reviews the privacy policy as needed or when changes occur and updates it accordingly to ensure it is consistent with the applicable laws, regulations, and appropriate standards. ✓

Privacy policy maintained

The company has established a privacy policy that uses plain and simple language, is clearly dated, and provides information related to the company's practices and purposes for collecting, processing, handling, and disclosing personal information. ✓

Data classification policy established

The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel. ✓

This Trust Packet was exported on Sun Sep 18 2022.

This Trust Packet was exported on Sun Sep 18 2022.