Security

Cloud Insights

NetApp
April 18, 2022

Table of Contents

Security

Cloud Insights Security

Product and customer data security is of utmost importance at NetApp. Cloud Insights follows security best practices throughout the release life cycle to make sure customer information and data is secured in the best possible way.

Security Overview

Physical security

The Cloud Insights production infrastructure is hosted in Amazon Web Services (AWS). Physical and environmental security-related controls for Cloud Insights production servers, which include buildings as well as locks or keys used on doors, are managed by AWS. As per AWS: “Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff utilize multi-factor authentication mechanisms to access data center floors.”

Cloud Insights follows the best practices of the Shared Responsibility model described by AWS.

Product security

Cloud Insights follows a development lifecycle in line with Agile principles, thus allowing us to address any security-oriented software defects more rapidly, compared to longer release cycle development methodologies. Using continuous integration methodologies, we are able to rapidly respond to both functional and security changes. The change management procedures and policies define when and how changes occur and help to maintain the stability of the production environment. Any impactful changes are formally communicated, coordinated, properly reviewed, and approved prior to their release into the production environment.

Network security

Network access to resources in the Cloud Insights environment is controlled by host-based firewalls. Each resource (such as a load balancer or virtual machine instance) has a host-based firewall that restricts inbound traffic to only the ports needed for that resource to perform its function.

Cloud Insights uses various mechanisms including intrusion detection services to monitor the production environment for security anomalies.

Risk Assessment

Cloud Insights team follows a formalized Risk Assessment process to provide a systematic, repeatable way to identify and assess the risks so that they can be appropriately managed through a Risk Treatment Plan.

Data protection

The Cloud Insights production environment is set up in a highly redundant infrastructure utilizing multiple availability zones for all services and components. Along with utilizing a highly available and redundant compute infrastructure, critical data is backed up at regular intervals and restores are periodically tested. Formal backup policies and procedures minimize the impact of interruptions of business activities and protects business processes against the effects of failures of information systems or disasters and ensures their timely and adequate resumption.

Authentication and access management

All customer access to Cloud Insights is done via browser UI interactions over https. Authentication is accomplished via the 3rd party service, Auth0. NetApp has centralized on this as the authentication layer for all Cloud Data services.

Cloud Insights follows industry best practices including “Least Privilege” and “Role-based access control” around logical access to the Cloud Insights production environment. Access is controlled on a strict need basis and is only granted for select authorized personnel using multi-factor authentication mechanisms.

Collection and protection of customer data

All customer data is encrypted in transit across public networks and encrypted at rest. Cloud Insights utilizes encryption at various points in the system to protect customer data using technologies that includes Transport Layer Security (TLS) and the industry-standard AES-256 algorithm.

Customer deprovisioning

Email notifications are sent out at various intervals to inform the customer their subscription is expiring. Once the subscription has expired, the UI is restricted and a grace period begins for data collection. The customer is then notified via email. Trial subscriptions have a 14-day grace period and paid subscription accounts have a 28-day grace period. After the grace period has expired, the customer is notified via email that the account will be deleted in 2 days. A paid customer can also request directly to be off the service.

Expired tenants and all associated customer data are deleted by the Cloud Insights Operations (SRE) team at the end of the grace period or upon confirmation of a customer’s request to terminate their account. In either case, the SRE team runs an API call to delete the account. The API call deletes the tenant instance and all customer data. Customer deletion is verified by calling the same API and verifying that the customer tenant status is “DELETED.”

Security incident management

Cloud Insights is integrated with NetApp’s Product Security Incident Response Team (PSIRT) process to find, assess, and resolve known vulnerabilities. PSIRT intakes vulnerability information from multiple channels including customer reports, internal engineering, and widely recognized sources such as the CVE database.

If an issue is detected by the Cloud Insights engineering team, the team will initiate the PSIRT process, assess, and potentially remediate the issue.

It is also possible that a Cloud Insights customer or researcher may identify a security issue with the Cloud Insights product and report the issue to Technical Support or directly to NetApp’s incident response team. In these cases, the Cloud Insights team will initiate the PSIRT process, assess, and potentially remediate the issue.

Vulnerability and Penetration testing

Cloud Insights follows industry best practices and performs regular vulnerability and penetration testing using internal and external security professionals and companies.

Security awareness training

All Cloud Insights personnel undergo security training, developed for individual roles, to make sure each employee is equipped to handle the specific security-oriented challenges of their roles.

Compliance

Cloud Insights performs independent third-party Audit and validations from external Licensed CPA firm of its security, processes, and services, including completion of the SOC 2 Audit.

Information and Region

NetApp takes the security of customer information very seriously. Here is how and where Cloud Insights stores your information.

What information does Cloud Insights store?

Cloud Insights stores the following information:

- Performance data

  Performance data is time-series data providing information about the performance of the monitored device/source. This includes, for example, the number of IOs delivered by a storage system, the throughput of a FibreChannel port, the number of pages delivered by a web server, the response time of a database, and more.

- Inventory data

  Inventory data consists of metadata describing the monitored device/source and how it is configured. This includes, for example, hardware and software versions installed, disks and LUNs in a storage system, CPU cores, RAM and disks of a virtual machine, the tablespaces of a database, the number and type of ports on a SAN switch, directory/file names (if Cloud Secure is enabled), etc.

- Configuration data

  This summarizes customer-provided configuration data used to manage customer inventory and operations, e.g. hostnames or IP addresses of the monitored devices, polling intervals, timeout values, etc.

- Secrets

  Secrets consist of the credentials used by the Cloud Insights Acquisition Unit to access customer devices and services. These credentials are encrypted using AES-256, and the private keys are stored only on the Acquisition Units and never leave the customer environment. Even privileged Cloud Insights SREs are unable to access customer secrets in plain-text due to this design.

- Functional Data

  This is data generated as a result of NetApp providing the Cloud Data Service, which informs NetApp in the development, deployment, operations, maintenance, and securing of the Cloud Data Service. Functional Data does not contain Customer Information or Personal Information.

- User Access data

  Authentication and access information that allows NetApp Cloud Central to communicate with regional Cloud Insights sites, including data related to user Authorization.

- Cloud Secure User Directory Data

  In cases where the Cloud Secure functionality is enabled AND the customer chooses to enable the User

Directory collector, the system will store user display names, corporate email addresses, and other information collected from Active Directory.

User Directory data refers to user directory information collected by the Cloud Secure User Directory data collector, not to data about the users of Cloud Insights/Cloud Secure themselves.

No explicit personal data is collected from infrastructure and services resources. Collected information consists of performance metrics, configuration information and infrastructure metadata only, much like many vendor phone-homes, including NetApp auto-support and ActiveIQ. However, depending on a customer's naming conventions, data for shares, volumes, VMs, qtrees, applications, etc. may contain personally identifiable information.

If Cloud Secure is enabled, the system additionally looks at file and directory names on SMB or other shares, which may contain personally identifiable information. Where customers enable the Cloud Secure User Directory Collector (which essentially maps Windows SIDs to usernames through Active Directory), the display name, corporate email address and any additional attributes selected will be collected and stored by Cloud Insights.

Additionally, access logs to Cloud Insights are maintained and contain users' IP and email addresses used to log into the service.

Where is my information stored?

Cloud Insights stores information according to the region in which your environment is created.

The following information is stored in the host region:

- Telemetry and asset/object information, including counters and performance metrics
- Acquisition Unit information
- Functional data
- Audit information on user activities inside Cloud Insights
- Cloud Secure Active Directory information
- Cloud Secure Audit information

The following information resides in the United States, regardless of the region hosting your Cloud Insights environment:

- Environment site (sometimes called "tenant") information such as site/account owner.
- Information that allows NetApp Cloud Central to communicate with regional Cloud Insights sites, including anything to do with user Authorization.
- Information related to the relation between the Cloud Insights user and the tenant.

Host Regions

Host regions include:

- US: us-east-1
- EMEA: eu-central-1
- APAC: ap-southeast-2

More Information

You can read more about NetApp's privacy and security at the following links:

- Trust Center
- Cross-Border Data Transfers
- Binding Corporate Rules
- Responding to Third-Party Data Requests
- NetApp Privacy Principles