CLOUDPHYSICS

DATA-DRIVEN INSIGHTS FOR SMARTER IT

CloudPhysics Security FAQ

CloudPhysics has applied our extensive security expertise to ensure customer data is protected at all points of the data transactions. This document answers some of the most common security questions. For a more extensive discussion of our security procedures, please contact us.

Q. What is the CloudPhysics Observer?

CloudPhysics collects data from your environment using a virtual appliance called the CloudPhysics Observer. This virtual appliance is a minimum resource appliance designed to collect data from within your VMware vCenter and cloud environment through read-only APIs, process the data, and share the data to CloudPhysics through secure means.

Additional levels of data collection are available with elevated privileges for guest process discovery using VMware Tools APIs and limited guest credentials at the discretion of the vSphere Admin.

Q. What are the system requirements of the CloudPhysics Observer?

The virtual appliance requires the following resources:

8GB of RAM, 2 Virtual CPU's, and 20GB of disk space when deployed. Total network traffic resources will be approximately 5MB per hour per 100 VMs in the datacenter.

The CloudPhysics observer will also require internet access to send collected data to the public cloud through an encrypted connection to the internet domain:

entanglement.cloudphysics.com

This domain is used for API calls only and has no public accessible web pages.

These communications will occur on Port 443. The Virtual Appliance must be on a network LAN segment that has access to VMware vCenter for VMware vSphere data collection. Data collection for cloud providers will be collected directly by CloudPhysics from the public cloud through published APIs.

Q. Does CloudPhysics deploy any agents to hosts or VM guest operating systems?

CloudPhysics does not deploy any probes or agents to VMware ESXi Hosts or any guest OS. All communications are achieved through existing management interfaces and results in no additional load to the host environment. CloudPhysics can take advantage of VMware Tools to collect process details within a guest if already deployed but is not required for infrastructure data collection.

Q. How is Data Collected?

CloudPhysics Observer collects data from VMware vCenter and cloud providers by public APIs. For VMware vCenter, CloudPhysics collects performance, configuration, and other metadata from the VMware vCenter on a defined schedule. Natively, vCenter collects performance and configuration data from its managed resources on a 20-second granularity. This data is typically rolled-up and destroyed once data is an hour old by vCenter. Before data is rolled-up and destroyed, CloudPhysics collects this performance and configuration data frequently enough directly from vCenter to maintain the 20-second granularity. This data collection process is agentless and has no impact on the VMs or hosts being analyzed since it already exists in vCenter. For cloud providers, CloudPhysics collects configuration and performance history data from the public APIs once per day. For VMware vCenter, CloudPhysics requires a Read-Only account with access to list and read configurations of the virtual environment.

For VMware vCenter, these credentials are detailed in the CloudPhysics install guide located at https://www.cloudphysics.com/installing-cloudphysics/ and for Amazon Web Services, the policy details can be found at https://www.cloudphysics.com/connectaws/

Q. What type of data is Collected?

Infrastructure Configuration Data
This data describes either the virtual datacenter or the cloud environment under observation by CloudPhysics. This data defines the environment to be monitored including the vCenter and its configurations as well as the resources consumed by the systems and resources under management by vCenter. This data does not include network topology or data to recreate the network architecture. For VMware vCenter v4.0 and above, this data will consist of vCenter details, datacenter details, VM details, host details, virtual domain details, datastore details, network port details, virtual network details, and resource group details.

Performance Data
This data will consist of CPU, Storage, Network, and RAM usage details. Utilization, peak performance, bandwidth, and characteristics of these will all make up the performance data. CloudPhysics will also generate derivatives of this data for averages, means, 99th Percentile, and 95th Percentiles.

Event and Task Data
Event and Task data provides a view of major events and scheduled services in the environment such as resources starting and stopping, vMotions, and environmental changes. These events and tasks often include the event, a brief description, and the associated service or username that initiated the event.

Metadata and Tags
Many resources contain metadata to describe a service, its role, and provide context to its relationship to other objects in the environment. The most common metadata collected are tags used for managing objects in the environment to offer classification and organization of resources, data, and services.

Running Processes within VMware VMs
With the addition of the Fall 2018 Observer Refresh, CloudPhysics provides administrators the option to collect inventories of running processes within a VM. This data collection is achieved as a guest request through VMware tools and allows the VMware tools to return a list of processes currently running on the host to help classify applications and services associated with VMs.

Q. How long is data kept?

CloudPhysics will retain all metadata indefinitely for aggregated and anonymous statistical and historical trending analysis. This metadata is used to help compare users to the global data set to identify inefficiencies. Machine metadata can be deleted at the discretion of CloudPhysics.

Q. Where is my data stored?

Data collected by the observer is quickly processed and parsed to remove unnecessary data before being compressed, encrypted, and sent to the CloudPhysics servers for data processing. The most recent data collections will be held in the Observer until they can be delivered to the CloudPhysics cloud. CloudPhysics stores each customer's data in dedicated logical containers until the data can be queued, verified, and loaded into the CloudPhysics data lake for analysis.

Q. How is data protected in transit to the Cloud?

All data sent to CloudPhysics is compressed and encrypted before sending to the cloud. All communications to the cloud are secured with an TLS connection on Port 443. Authentication data is one-way hashed at rest. Access is controlled via AWS IAM, SSH public key auth, and firewalls. The current release of the CloudPhysics appliance utilizes TLS v1.2.

Q. Is any personal identifiable information collected?

CloudPhysics collects data center configuration and performance data. As a result, there is minimal exposure of personal identifiable information collected. CloudPhysics only collects user information for portal account access and invitations of new users by existing users. This data will consist of company, name, and email address only. Within the data collected from the customer environments, the only places a user ID may be observed in the data is for events within the environment such as snapshots, vMotions, or environmental changes. This data carries no other user association to data at CloudPhysics.

Q. How is my data secured in the cloud?

Unique pseudo-random hashed identifiers are created to represent each organization. The metadata is processed/stored in Amazon Web Services in a multi-tenant structure. AWS data security services are detailed at https://aws.amazon.com/security/ and https://aws.amazon.com/compliance/. Strict firewall rules and two-factor authentication are used to limit access to customer data.

Q. Who has access to my data?

Authorized CloudPhysics employees, the customer and anyone external authorized by the customer. CloudPhysics' third parties and contractors do not have access to our production environment.

Q. How does CloudPhysics mitigate vulnerabilities and data risk?

CloudPhysics monitors security vulnerability disclosures and maintains our environment accordingly. Full disk encryption is mandated for all employee computers and mobile devices that have access to CloudPhysics documents/data. Administrative access is via two-factor authentication (SSH public key with password-protected keys).

Q. How does CloudPhysics use the data that it collects?

Beyond providing analytics and assessments to the end users, CloudPhysics will anonymize and aggregate some metadata metrics to produce statistical models to provide trends as a global dataset. Statistical models are used to allow customers to compare their own utilization and efficiency against the global dataset.

Q. Who has access to the data collected in my environment?

Customers who use CloudPhysics may assign an administrator who can manage access to all customer data. User and partner management pages within the platform allow the customer to control and limit access to data. Some data is aggregated and anonymized for the purpose of analytics and reporting as defined in the terms of service.

Q. Does CloudPhysics share the data it collects?

CloudPhysics does not share customer data with third parties without authorization by the user. Customer data is only available to the customer, customer authorized third parties, or under other contractual terms of service for specialized assessments approved by the customer.

Vendors, Suppliers, and OEM's
CloudPhysics' Services uses Personal Information for internal and service-related purposes only and may provide it to third parties to allow CloudPhysics to offer CloudPhysics' Services. For example, CloudPhysics may share billing and credit information with service providers for the purposes of processing credit card transactions.

As Required By Law and Similar Disclosures
We may access, preserve, and disclose your Personal Information, other account information, and content if we believe doing so is required by law or if those actions are reasonably necessary to:

- Comply with legal processes, such as a court order or subpoena
- Enforce this Privacy Policy or our End User Agreement;
- Respond to claims that any content violates the rights of third parties;
- Respond to your requests for customer service;
- Respond to law enforcement;
- Investigate and prevent unauthorized transactions or other illegal activities; or
- Protect our or others' rights, property, or personal safety.

Merger, Sale, or Other Asset Transfers
We may disclose information we possess about you as part of a merger, acquisition, sale of company assets, or transition of service to another provider, as well as in the unlikely event of insolvency, bankruptcy, or receivership in which your Personal Information would be transferred as one of the business assets of the company. We do not guarantee that any entity receiving such information in connection with one of these transactions will comply with all terms of this Privacy Policy.

To Others Within Your Organization or with Your Permission
After a person demonstrates proof of membership to a certain organization, we may disclose to that person the names of that organization's members who have evaluated or purchased our service. We may also disclose your Personal Information with your permission.

Q. When is my data deleted?

CloudPhysics does not delete data. Metadata is maintained, aggregated, and anonymized to provide trend analysis of the larger set of data over time. Organizations who wish that their data be explicitly deleted can submit a formal request for account deletion by email to support@cloudphysics.com

Q. How large of an environment will CloudPhysics support?

CloudPhysics is not limited to the number of VMs, Hosts, Servers or Clouds. The current cloud model allows for one CloudPhysics Observer per vCenter to allow scalability. Data sent to the cloud will queue for processing and the environment will scale dynamically to accommodate capacity.

Q. How is the Observer secured and how often is it updated?

The CloudPhysics Observer is a hardened guest. All unnecessary services, packages and users have been removed. Collection code runs in separate process and network namespaces from the base appliance and these namespaces are deleted and recreated from an immutable base image on each reboot of the appliance.

Q. How does CloudPhysics monitor availability and integrity of hosts within our environment?

CloudPhysics does not monitor the availability of systems within the customer organizations beyond the most recent communication between the CloudPhysics Observer and CloudPhysics cloud services. We utilize internal and third party services to monitor availability and functioning of hosts within our infrastructure.

Q. What credentials are required to be granted to CloudPhysics to access the vCenter?

CloudPhysics needs a limited access account that has read and list capabilities against VMware vCenter. Details for security and policy requirements for vCenter are detailed at https://www.cloudphysics.com/installing-cloudphysics/

Q. For AWS analysis of instances, what credentials are required?

CloudPhysics require limited list and describe rights to AWS services for EC2, AutoScaling, CloudWatch, S3, and billing. These policies and steps to configure are located at https://www.cloudphysics.com/connectaws/

Q. What connectivity and protocols are used by the Observer?

CloudPhysics communicates over TLS 1.2 for current observers on Port 443 from the CloudPhysics Observer to CloudPhysics. Communications to Amazon Web Service will occur over secure REST API communications on TLS and HTTP on Port 443. All communications are encrypted using the latest supported secure standards for data communications.

Q. How do I grant or manage access of my data to my Partners and Resellers?

Administrators can invite new users, disable current users, and change permissions of current users. Under some assessments, terms of services may require that partners maintain access to the customer account for the duration of the assessment. Account administrators can manage user access through the User Manager page within the CloudPhysics portal at https://app.cloudphysics.com/management/user

Q. What browsers are supported by CloudPhysics?

CloudPhysics currently only officially supports Google Chrome Browser. All pages are designed to support HTML5 compatible browsers and as such HTML5 browsers should be compatible with CloudPhysics dashboards. Microsoft Internet Explorer is not supported.

Q. How will CloudPhysics respond to a security incident?

CloudPhysics classifies a customer-specific security incident as any incident that meets any one of the following conditions.

- Any customer data has been exposed to a third party not authorized by the customer as defined in the Terms of Services.
- Any data has been downloaded by a third party not authorized by the customer or as defined in the Terms of Service.
- An unauthorized data breach or event has taken place in the CloudPhysics data and application hosting environment that impacts customer identity or data.

Should one of these events occur, CloudPhysics will communicate the event to the primary account contact immediately. Further analytics of the exposed data and services will be assessed to determine the full scope of impact. If CloudPhysics is aware of the recipient of the data, it will communicate the name of the third party, the time-frame, and scope of data exposed. CloudPhysics will continue its analysis to resolve any application, platform, or procedural changes that will be necessary to remediate the issue.

Q. What is CloudPhysics current Privacy Policy?

CloudPhysics maintains the current Privacy Policy at https://www.cloudphysics.com/privacy-policy/

Q. What is CloudPhysics current Cookie Policy?

CloudPhysics maintains the current Cookie Policy at https://www.cloudphysics.com/cookie-policy/

Q. What are the CloudPhysics Terms of Use?

CloudPhysics maintains the current Terms of Use at https://www.cloudphysics.com/terms-of-service/

Q. Is CloudPhysics GDPR Compliant?

CloudPhysics established GDPR guidelines for user opt-in, deletion, and data request requirements in March 2018. CloudPhysics adheres to GDPR regulations as it applies to the data used and limits user data tracking and marketing with such data. CloudPhysics uses minimal identifiable data tracking. By agreeing to use the platform, the users agree to associate their email address, name, and company to an account. The core application for CloudPhysics does not collect any more personal information than this. All of our cookie and activity data is treated as anonymous and used solely for session management (Load balancer), volume tracking, and site activity. Users are presented with a Cookie tracking notification on first visits and this is audited with OneTrust. The public portal may collect customer feedback and requests and maintain this data for communication purposes.

Users have the right to request data be deleted or reviewed as defined in the Privacy and Cookie Policies. Users who choose to have their profile and data deleted must provide proof of identity before deletion as detailed in the Privacy Policy. Since some personal data is used for audit and billing, this data will be retained. SalesForce data is maintained for account audit and deal management purposes for CloudPhysics and Partners. Users invited by Partners through the platform are not tracked and no data is used until the users accept an invitation. Some data may be collected as invites by third party partners inviting new users. This collection will be limited only to email address. This data is periodically purged from the system if the invite is not accepted and is not used for other purposes.

CloudPhysics continues to enhance our services and user management as more services become available through our partners to maintain our GDPR Compliance. With the focus on collecting data center metadata, CloudPhysics already limits risk as it does not manage user contacts beyond the basic user account data and user invitation data. Customer data is collected as an Opt-In model for account enrollment.

For international users, by choosing to visit CloudPhysics' Services or otherwise providing information to us, you agree that any dispute over privacy or this Privacy Policy will be governed by California law.

If you are visiting from the European Union or other regions with laws governing data collection and use, please note that you are agreeing to the transfer of your Personal Information to the United States to us. By providing your Personal Information, you consent to any transfer and processing in accordance with this Policy.

You also consent to the adjudication of any disputes arising in connection with us or CloudPhysics' Services in accordance with the Terms of Service, as applicable.

Guest Process and Application Discovery Questions

Q. Am I required to configure the guest process collection or dependency mapping collection?

No. Data collection within guest operating systems is entirely optional and definable during the CloudPhysics Observer installation and configuration.

Q. Can I disable guest process collection and network dependency mapping?

Yes. Dependency mapping and guest process collection are options that require dedicated credentials during the setup of the CloudPhysics Observer. If no credentials are provided, the collection process will not be executed.

Q. How are the guest processes collected?

Guest processes are collected with a VMware Tools feature to collect guest processes. This request originated from the CloudPhysics Observer to VMware vCenter. Upon request, vCenter will attempt to issue the command to the VMware tools within the guest OS. The VMware vCenter will initiate a process collect command under the identity of the guest account specified in the CloudPhysics observer during the Observer setup process. The VMware Tools will issue the command as the specified guest user every six hours. If the guest OS allows the guest user, the process list from the host is collected and stored in a guest user home directory. Upon completion of the collection, Output of command execution is collected by CloudPhysics Observer using vSphere API that in turn uses VMware tool to collect the command output temporarily stored in the output file.

Assuming user have access to their own home directory, the application data will be written to the user home directory and removed upon data collection. If the user does not have sufficient rights to delete their temp files, the file will be overwritten with each collection to ensure the volume storage is minimal.

Q. How is dependency mapping data collected?

Dependency Mapping is derived from a network analysis tool called NetStat. CloudPhysics issues a request to VMware vCenter for details form the guest OS. VMware vCenter can direct queries to the guest OS if VMware Tools is deployed and enabled. The request will be a simple command to issue a NetStat command and direct the output to a temporary file located in the guest user's home directory. The NetStat command will collect all open network communications and report the source IP Address, Destination IP Address, TCP/UDP, as well as port. This data is directed into a local temp storage file where it is processed and sent to the VMware vCenter by VMware Tools.

Q. How frequently is my data collected?

CloudPhysics will collect both guest process and network dependency data independently on a defined schedule. Initial releases will collect data every six hours.

Q. How do you create a dependency map?

Dependency maps are generated based on source and destination IP Address and ports identified by NetStat during the dependency mapping data analysis online. These data will identify all major network communications by the guest OS and map IP addresses to other VMs. Any VM that talks outside of the private network ranges would be considered communications outside of your data center.

Q. What credentials are required to collect guest processes and Dependency Data?

A domain guest ID is best for collection of data. This user credential does not need to be a domain admin or have root access within a guest OS. For mixed environments, ensure the same user id and password exists in both Linux and Windows environments.

Q. What data is collected for guest process?

A simple table of process ID and Process Name is generated when the vSphere API command is issued. This command returns back a simple text list of all processes currently running in the guest OS.

Q. What data is collected for Dependency mapping?

NetStat returns a text output of the source, destination, port, and potentially protocol information from the guest. This data varies slightly from the operating system to operating systems but typically. Additional data may include packet count, state, or world ID.

Q. What is the data flow during collection?

CloudPhysics issues a request for data to VMware VCenter for a specific guest OS. VMware vCenter will issue the credential and command to the guest OS. If the command is allowed to execute, VMware tools will direct all output from the command to a temp file in a guest user home directory. Upon completion of the command, VMware tools retrieve the temp file and direct the output back to VMware vCenter as a temporary variable for the guest OS. CloudPhysics will then collect the temp variable from the VMware vCenter on the next data collection cycle. If the data collection fails or an error is generated, this data is also reported back to the VMware vCenter for collection by the CloudPhysics observer.

Q. How long is my data kept?

All data will be retained indefinitely for a user account to allow for historical analysis by the users. This data will remain part of your account as long as your account is active and will not be deleted until a deletion request is received.

Q. Who will have access to the guest process and dependency mapping data?

All users with access to your CloudPhysics account will be able to use analytics that derives data from the data collection process. The Processes will be used as tags in the CloudPhysics environment to allow for quick classification of applications and guest OS instances. NetStat Dependency mapping data will only be available through Dependency Mapping cards that are enabled to account users.

Q. Can I remove or delete my data?

All account data can be removed upon request to by sending an email to support@cloudphysics.com. CloudPhysics keeps all anonymized metadata for global comparison of performance, configurations, and is used to compare users against the global dataset.

Q. How do I access my guest process Data in the CloudPhysics portal?

CloudPhysics makes all guest process data available today in Card Builder for the VM Object called “guest processes”. In addition, some guest processes are used to generate tags or events for some analytics. Example: SQL Server processes is used to identify guest OS with SQL databases installed and can be used to automatically generate tags associated with these VMs.