TREND MICRO

SecureCloud™ 2.0

Private Security for the Public and Private Clouds

On-Premise

Administrator's Guide

Protected Cloud

How SecureCloud Works

SecureCloud provides a data encryption layer within a virtual machine image to decrypt your data in real-time after the appropriate credentials have been validated. Likewise, SecureCloud encrypts your data in real-time when putting the information back into data storage.

When the virtual machine image boots up, it uses the Runtime Agent to provide its credentials to SecureCloud and request an encryption and decryption key along with the appropriate information to connect to data storage. The SecureCloud Key Manager responds with a request for information pertaining to the environment which it will use to evaluate against policies that have been created for the specific device. For example, a policy can consist of rules to check that the virtual machine is in compliance to the IT policy regarding what network services should be enabled or pattern file version, and location of where the virtual machine is running to name a few. The integrity and credential information helps to ensure that the instance meets the policy criteria set by the administrator in order to run certain applications, and ensures that the environment is safe to release the encryption key into based on the policy criteria.

SecureCloud provides and maintains your encryption keys, either locally or through a KMIP server. The virtual machine image does not store encryption or decryption keys. SecureCloud also provides other management capabilities such as reporting and auditing functions.

For the SecureCloud On-Premise product, you need to complete two installations. First, you need to install the SecureCloud Management Server and then install the SecureCloud Runtime Agent.

SecureCloud On-Premise is set up and maintained through the Central Management Console. This console is where you specify the settings necessary to use the main functionality of SecureCloud On-Premise, which is done through the Web Console. In

order to use the Web Console, you must open the Central Management Console and specify the activation code to activate your license and configure your SMTP server in order to receive system alerts.

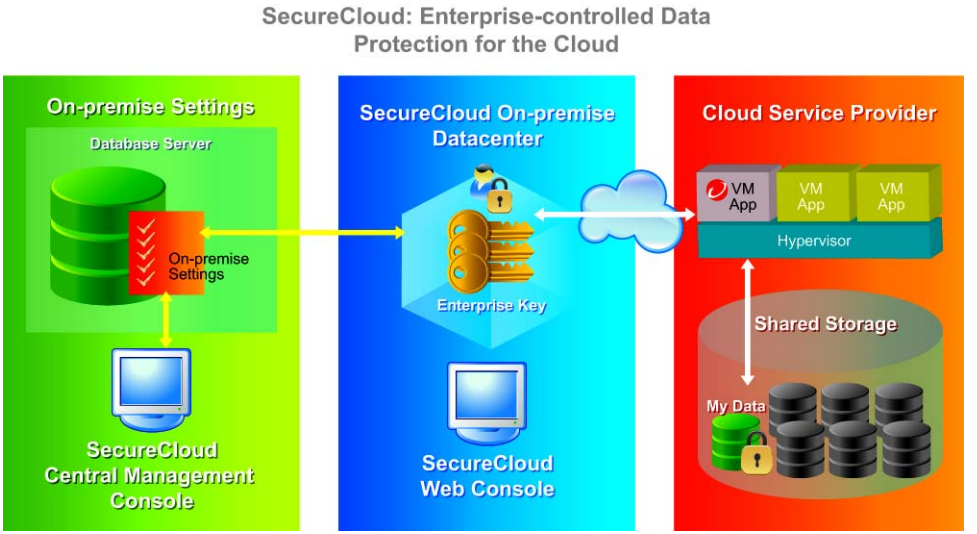

FIGURE 1-1. How SecureCloud On-Premise functions

You access SecureCloud through the secure Web Console. Using this portal, you define the criteria on which instances can receive encryption/decryption keys. For example, criteria can include the location of the application, host name, the latest operating system patch, and/or the latest Trend Micro engine and pattern file. In addition, you can get report and audit information about your account using the portal.

SecureCloud Interaction with the vCloud API

The vCloud API is used by SecureCloud to determine the identity of a machine image in the vCloud environment. The Configuration Tool uses the vCloud API to learn what data storage devices in the vCloud environment are available for encryption.

The SecureCloud Runtime Agent uses the vCloud API to learn the identity and integrity of the vCloud machine image. This information is retrieved from the vCloud API and sent to the Management Server where the user can either grant or deny an encryption key to the requesting machine image, based on the identity and integrity credentials of the vCloud machine image.

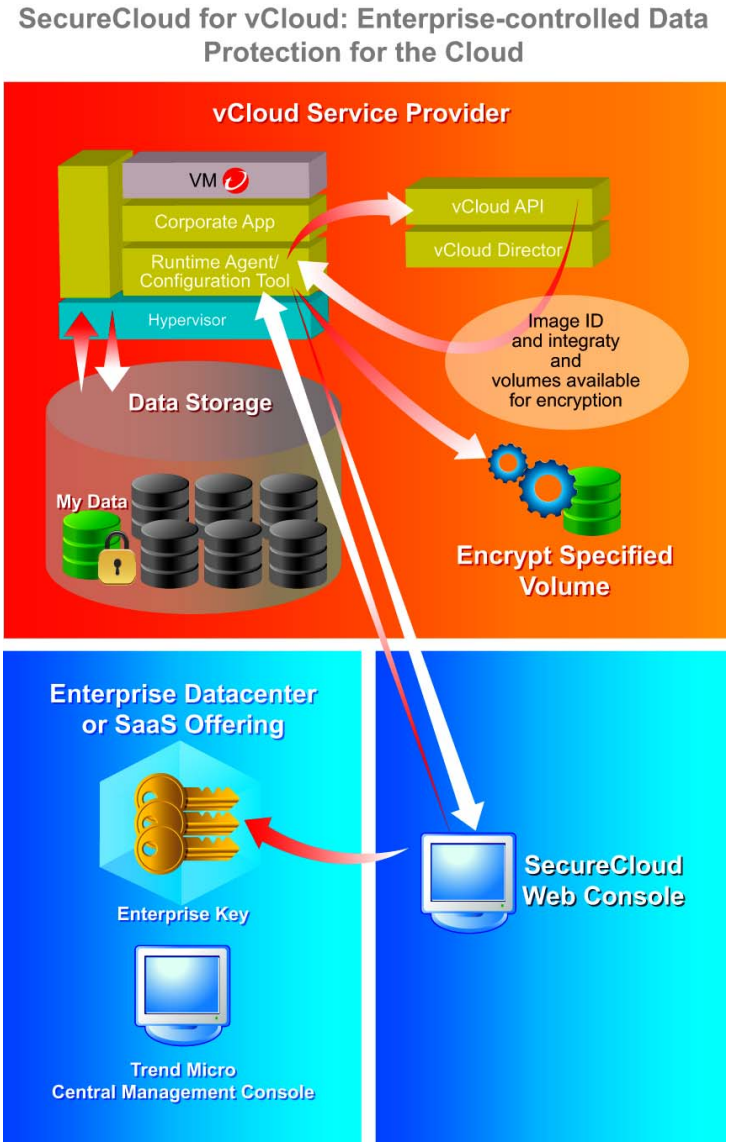

FIGURE 1-2. How SecureCloud functions in the vCloud Environment

Basic Components of SecureCloud

Runtime Agent

The SecureCloud Runtime Agent is the software module that is installed with your virtual machine image in your cloud service provider's environment. The Runtime Agent provides the following functionality:

- Checks the integrity of the cloud environment against the rules set in the SecureCloud policy for the specific virtual machine and device
- Mounts a configured encrypted data storage device
- Establishes an SSL session with the SecureCloud key manager
- Establishes a private session with a separate session key over SSL. This is performed in case the SSL connection is compromised. In doing so, even if the SSL session is compromised the communication between the agent and key server is still encrypted.
- Authenticates the communication between the Runtime Agent and Key Manager using Message Authentication Code.
- Creates and tears down an encrypted area on the virtual machine storage in order to store the cloud service provider's credentials

Configuration Tool

The Configuration Tool is part of the SecureCloud Runtime Agent. After product installation, you can launch the Configuration Tool from the installation wizard. If you decline to run the Configuration Tool at this time, you can launch it later.

The Configuration Tool configures the following:

- Cloud service provider and cloud service provider plugin
- Cloud service provider's credentials (includes the rotation of credential keys for Amazon environment)
- SecureCloud account ID
- Web Service API URL
- Device information for the running machine instance
- Device encryption

Management Server

The Management Server hosts the key approval process, log collection and reporting.

The SecureCloud Web Console is the Graphical User Interface (GUI) front end to the Management Server. Your interaction with the SecureCloud Web Console is based on role-based administration and privilege levels. The Management Server allows for multiple users, having varying user roles (see *User Roles* on page 7-7).