


Effective End-to-End Cloud Security

Securing Your Journey to the Cloud

 Trend Micro™
SecureCloud

*A Trend Micro & VMware White Paper
August 2011*



I. EXECUTIVE SUMMARY

This is the first paper of a series of two and will focus on how VMware and Trend Micro products work together to provide a cloud security solution. This paper will provide a summary, overview, and architectural diagrams of VMware vCloud™ Director and Trend Micro™ SecureCloud solution.

Just as the personal computer and networking revolutionized the way we go about day-to-day life and conduct business, so too is cloud computing revolutionizing society again. Cloud computing places virtually limitless computing power in the hands of anyone who has access to it. There are different service models of cloud computing, including; public cloud, private cloud, hybrid cloud, and community cloud. Each of these cloud computing models offers certain functionality and features depending on the requirements of an organization. For example, a hybrid cloud model could combine a private cloud, which is augmented with compute capacity from one of more public clouds. This model is effective in providing capacity on a temporary basis to handle spikes in load—also referred to as cloud-bursting.

To quote Uncle Ben from the movie Spiderman “with great power comes great responsibility.” Although cloud computing most certainly provides great power through an approach that leverages the efficient pooling of on-demand, self-managed virtual infrastructure, it also poses great opportunity to organized crime. A single vulnerability can expose thousands of tenants’ information hosted by a cloud provider.

Providing security for sensitive data in the cloud is a complex and critical task for any organization. Further, privacy concerns continue to generate regulations that hold data owners accountable for breaches and misuse. One method used to provide protection from the risks associated with deploying sensitive information into the cloud is encryption. Applying strong and proven encryption techniques like the Advanced Encryption Standard (“AES”) to cloud deployments protects data by making it indecipherable to anyone who doesn’t have access to the encryption key. An additional level of cloud security may be achieved by storing the encryption keys physically separate from the cloud service provider, thus ensuring clear segregation of duties between the cloud provider and the owner of the data. Trend Micro offers this level of cloud protection through its SecureCloud solution.

Trend Micro™ SecureCloud provides data protection and encryption key management for public cloud, private cloud, hybrid cloud, and community cloud environments. Data is encrypted on a virtual machine before being written to any SCSI, iSCSI, NFS, or IDE storage device and decrypted when read back. The symmetric keys for the encryption process are managed by the SecureCloud Key Manager—which is available as a hosted service from Trend Micro or can be installed within your own data center. SecureCloud’s unique policy-based key management allows it to ensure that encryption keys are released only into safe cloud environments via identity and integrity checks. This is achieved by applying numerous rules to key release decisions, such as checking which network services are running within the virtual machine; which helps SecureCloud assess the cloud environment’s identity and integrity.



II. CLOUD SECURITY BASICS

DYNAMIC VIRTUAL MACHINES: VM SECURITY STATE AND SPRAWL

Virtual machines are dynamic. They can quickly be reverted to previous instances, paused, and restarted very easily. They can also be readily cloned and seamlessly moved between physical hosts. This dynamic nature increases the potential for VM sprawl, which makes it difficult to achieve and maintain consistent and effective security practices. Vulnerabilities or configuration errors may be unknowingly propagated and it is difficult to maintain an auditable record of the security state of virtual machines over time. Because of the fluid nature of cloud computing environments, enterprises do not always know who they are sharing hardware with—it could be a tenant consuming extra hardware resources that slow your operations, or it could be a tenant that is malicious in nature. This uncertainty drives the need to prove the security state of a system, regardless of its location or proximity to other, potentially insecure virtual machines.

VULNERABILITY EXPLOITS AND VM-TO-VM ATTACKS

In many cases the physical servers providing the platform for cloud computing use the same operating systems, enterprise, and web applications as localized virtual machines and physical servers. The ability for an attacker or malware to remotely exploit vulnerabilities in these systems and applications is a significant threat to virtualized cloud computing environments. In addition, the multi-tenant nature increases the attack surface and risk of VM-to-VM compromise. Intrusion detection and prevention systems must be able to detect malicious activity at the virtual-machine level, regardless of the location of the VM within the virtualized cloud environment.

DATA MOBILITY: ACCESS CONTROL

To ensure high availability of services, data is replicated within virtualized and cloud infrastructures. As job functions and responsibilities change, so too do access control requirements. There is always a significant threat of user and application configuration errors; data can easily be exposed to those who should not have access to it. Insider threats also put sensitive information at risk to breach, manipulation, and theft.

III. TRENDMICRO AND THE VMWARE RELATIONSHIP

Trend Micro has a deep rooted relationship with VMware; as one of the first security vendors to use the VMware EPSec VMSafe API, Trend Micro's relationship builds on a strong foundation. Trend Micro has also engaged very closely with VMware to support vCloud Director, VMware's cloud computing product. The result is that SecureCloud is being supported with vCloud Director, and thus ensuring organizations that deploy vCloud Director for their public cloud, private cloud, hybrid cloud, or community cloud can take advantage of encryption in their cloud environment.

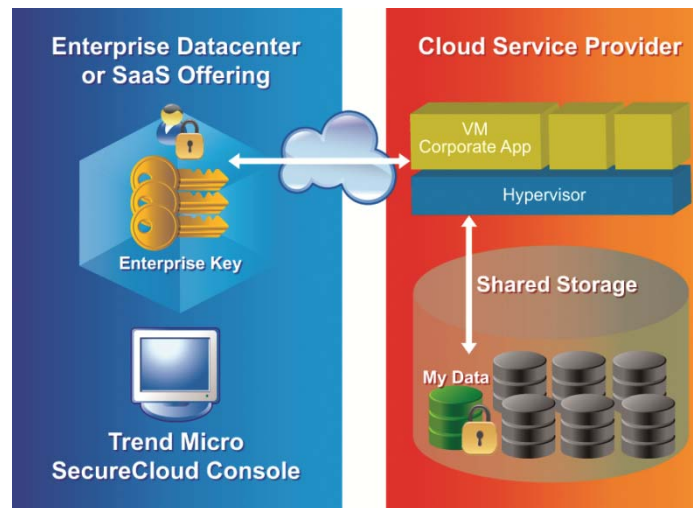


EFFECTIVE END-TO-END CLOUD SECURITY: TREND MICRO SECURECLOUD

IV. PROVIDING SECURITY IN THE TREND MICRO AND VMWARE ENVIRONMENT

SecureCloud provides a data encryption layer within a virtual machine image to decrypt customer data in real-time after the appropriate credentials have been validated. Likewise, SecureCloud encrypts customer 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 key along with the appropriate information to connect to data storage. For example, a virtual machine image could be required to report items like malware pattern file version, last full scan, network services, and location of the instance to SecureCloud during the request. This identifying information helps to ensure that the instance meets security and environmental criteria set by the administrator in order to run certain applications. Data is only decrypted within the virtual machine; this ensures that data at rest within or traversing the cloud infrastructure remains encrypted at all times.



SecureCloud generates and manages your encryption keys. Further, the virtual machine image does not store encryption keys when the image is not in use. SecureCloud also provides other management capabilities such as reporting and audit functions.

As a SaaS offering, SecureCloud provides a multi-tenant environment where multiple organizations are served. You access the SecureCloud portal through a secure Internet connection. Using this portal, you define the criteria on which instances can receive encryption keys and gain access to secure data. In addition, you can get report and audit information about your account using the portal.



V. 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 SecureCloud Runtime Agent provides integrity checking functionality such as IP address and location and uses Advanced Encryption Standard (AES) as the encryption standard to encrypt the volume using VM-Level encryption.

The Configuration Tool resides in your Cloud Service Provider's environment as part of the 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 virtualization plugin
- Cloud service provider's credentials
- SecureCloud account ID
- Web Service API URL
- Device information for the running machine instance
- Device encryption

MANAGEMENT SERVER

Trend Micro SecureCloud is offered in multiple delivery models, you can either use the hosted services delivered by Trend Micro, or deploy your own SecureCloud Management Server on-premise within your own datacenters. Trend Micro hosted services provide the SecureCloud Management Server with multi-tenant capability. The Management Server hosts the key approval process, log collection, and reporting.

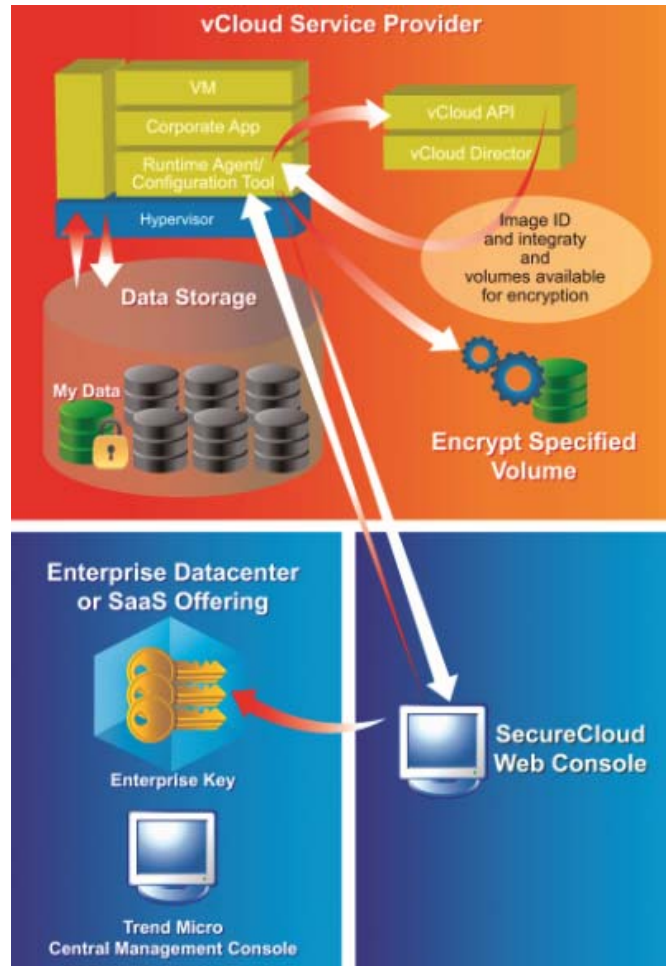
The SecureCloud Web console is the Graphical User Interface (GUI) front end to the Management Server. Your interaction with the SecureCloud Web console is based on role-based administration and privilege levels. The Management Server allows for multiple users, having varying user roles.

VMWARE VCLOUD API

The vCloud API is the primary way for customers, partners, and ISVs such as Trend Micro to integrate with the vCloud Director product.

➔ EFFECTIVE END-TO-END CLOUD SECURITY: TREND MICRO SECURECLOUD

The vCloud API is used by SecureCloud to determine the identity of a machine image in the vCloud environment. The vCloud API is also used by SecureCloud 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.

The vCloud API is an extremely important element of SecureCloud; it is utilized by the SecureCloud Runtime Agent configuration tool to gather information about what data storage devices in the vCloud environment are available for encryption, as these products and technologies evolve this will only increase.



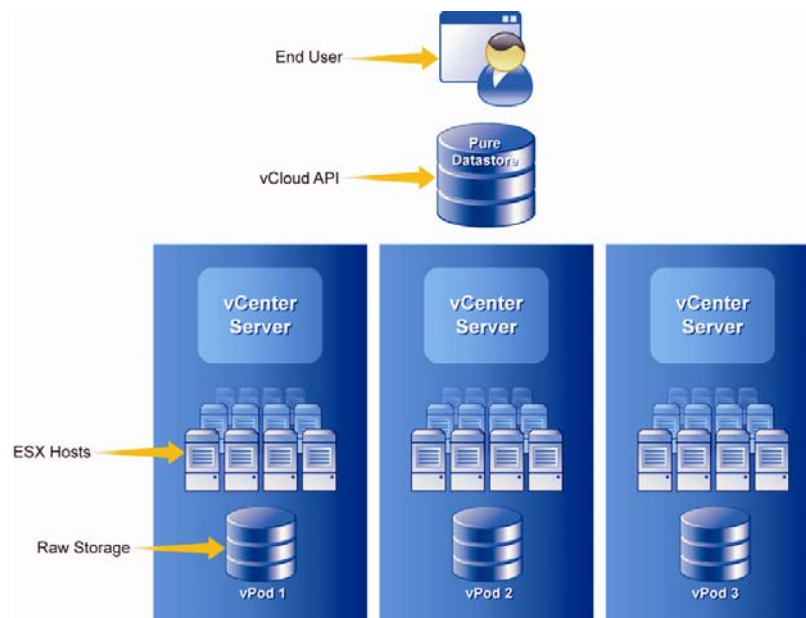
EFFECTIVE END-TO-END CLOUD SECURITY: TREND MICRO SECURECLOUD

VI. TREND MICRO AND VMWARE SERVICE PROVIDER CLOUD OFFERING

vCloud Director and the vCloud API enable service providers and enterprise customers alike to offer cloud-computing services that allow users to create entire data centers of virtual machines in the cloud. For example, the Open Virtualization Format (OVF) is the open standard that is used when creating virtual machines and vApps, which are composed of one or more virtual machines. It is the vCloud API that is used as the standard for provisioning and controlling these applications in the cloud.

What is really significant and important here is that the vCloud API deals entirely in terms of virtual entities without the need to configure and even reference the underlying physical infrastructure. For example, operations such as the configuration of storage and networking are all very complex operations and are handled by the VI Management API (VIM), which is an interface specification defined by the WSDL standard.

Here is an example that illustrates the vCloud API and how it operates at a Pure Virtual level.

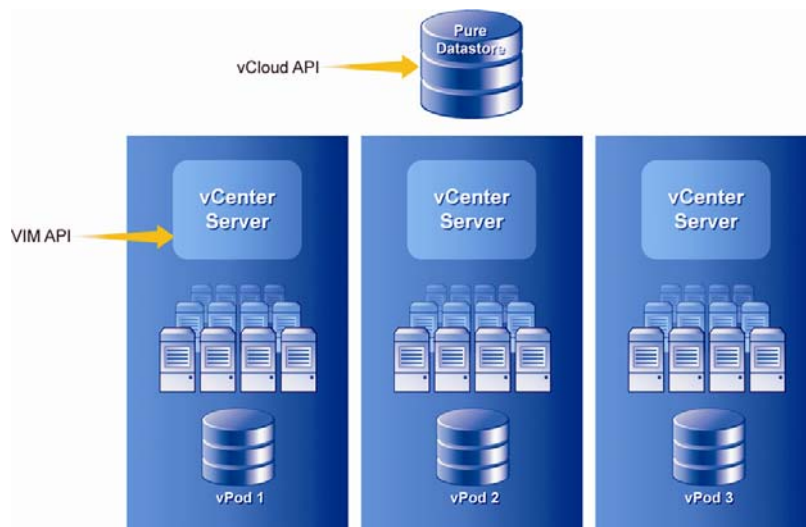


As you can see in the diagram we have the raw resources at the bottom and Pure Virtual resources on the top next to the end user. The same thing happens with networking, CPU, and memory. This is what makes the VMware vCloud API different. If you want to operate on Pure Virtual objects in the cloud then you would use the VMware vCloud API. If you in turn want to change around port group settings or storage configurations, etc. then you would need to use the traditional VI Management API (VIM) that exists today.



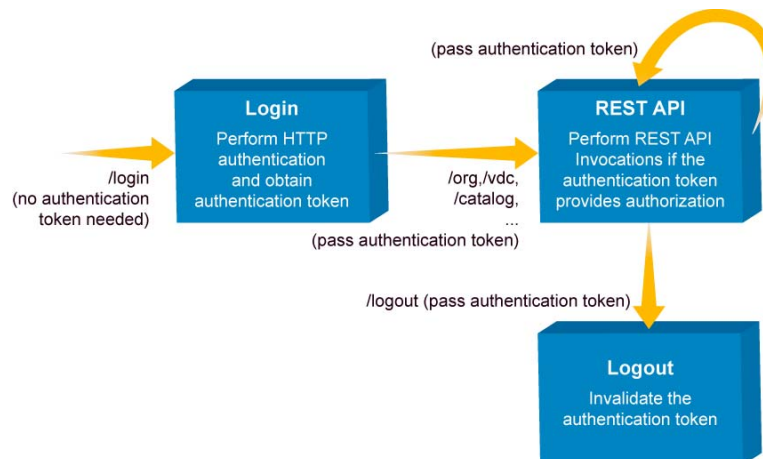
EFFECTIVE END-TO-END CLOUD SECURITY: TREND MICRO SECURECLOUD

It should be noted that the representation and externalization of the vCloud API is only available as part of VMware's vCloud Director product.



Another important aspect to the vCloud API is the security. With security in mind, the vCloud API has been designed and implemented with an access model that represents a **User API**, which provides a pure virtual REST API focused on self-provisioning and the use of OVF for VMs and vApp configuration and reconfiguration. An **Admin API** provides pure virtual REST APIs targeted at and used by System Organization administrators. And **Admin API Extensions** include all VMware specific REST APIs targeted to system administrators who want to build in extensibility. Another important aspect of the vCloud API is that VMware has submitted its vCloud API specification to the DMTF and is the lead on the work going on with OVF.

Here is an example of the vCloud API in action:





VII. THE TREND MICRO AND VMWARE KEY FEATURES TABLE

vSphere and vCloud API Protection & Control	
Threat Protection	<ul style="list-style-type: none"> Checks existence of Trend Micro security software providing intrusion detection and prevention, firewall, integrity monitoring, log inspection, and anti-malware capabilities. Ensures privacy amongst tenants by creating segregation through encryption. Provides the ability to adhere to compliance regulations by separation of duties. Uses industry proven AES encryption of the data to provide a robust data loss protection solution, securing intellectual property.
Access Control	<ul style="list-style-type: none"> Uses identity- and integrity-based policy enforcement to ensure only authorized virtual machines receive encryption keys. Enforces separation of duties with role-based management. Provides access to management console supported by major authentication standards, including Microsoft Active Directory, SAML 2.0, and leading identity and access management systems.
Privacy	<ul style="list-style-type: none"> Protects communication between Agent and Key Manager via AES 256 session keys. Does not store cloud provider credentials. Ensures data at rest remains encrypted at all times. Protects residual data remaining on physical servers after volumes are vacated or hardware is retired.
vSphere and vCloud API Abstraction & Management	
API Lifecycle	<ul style="list-style-type: none"> Uses the Web UI to reflect the vCloud inventory, providing intuitive encrypted vCloud Disk management. Automatically supports API versioning, including rollback to previous version.
Orchestration	<ul style="list-style-type: none"> Bases policy-driven API control on environment metadata. Controls storage availability based on environment integrity with user-defined policies. Supports vCloud Director 1.0 & 1.5 and vSphere, allowing for control of sensitive information throughout the virtualized infrastructure. Leverages vCloud's built in multi-tenancy to isolate customer data and session.
Protocols supported	<ul style="list-style-type: none"> Makes all API calls over HTTPS. Key Management API interfaces are only available over HTTPS.
High Availability	<ul style="list-style-type: none"> Architected as a horizontally scalable solution offering multiple front-end Key Managers.
Management API	<ul style="list-style-type: none"> Uses Management API to allow customers to integrate the solution into their customer facing portals, creating an intuitive customer experience.
Standards	
Supported standards	<ul style="list-style-type: none"> Includes SAML 2.0, REST, Microsoft Active Directory, XML 1.0



EFFECTIVE END-TO-END CLOUD SECURITY: TREND MICRO SECURECLOUD

VIII. CONCLUSION

Many of the risks that plague traditional computing are still prevalent in cloud computing. Cloud computing increases these risks because additional steps must be taken to ensure data protected. Instead of the customary security approach where external layered perimeters strategies are employed to protect sensitive data; Cloud computing requires a different approach. An inside-out approach, where the data is protected no matter where it is accessed from or replicated to as well as where the data is secured no matter where exists in the cloud.

Using solutions from Trend Micro and VMware enterprises can rest assured that access to their data is controlled from multiple levels through user access control principles provided by vCloud Director and virtual machine access control principles provided by SecureCloud.

Security Challenge in Virtualized Environment	Solution Benefit
Instant-On Gaps	<ul style="list-style-type: none"> Provides automatic protection until IT can install anti-virus Ensures always current antivirus patterns through centralized deployment in a virtual appliance
Resource Contention	<ul style="list-style-type: none"> Maintains consolidation ratios by reclaiming memory Prevents anti-virus storms with centralized scanning
IT Compliance Challenges	<ul style="list-style-type: none"> Maintains a single function per server to address PCI DSS and other regulations Provides visibility through introspection Logs vSphere, Deep Security events Enables separation of duties
Management Complexity	<ul style="list-style-type: none"> Streamlines anti-virus management Requires no retraining of administrators
Security Risks with Legacy Antivirus	<ul style="list-style-type: none"> Eliminates the target of attack Eliminates vulnerabilities to common attack methods

©2011 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [WP01_CloudSecurity_110812US]