Reference Testing Procedures for Trend Ready Verification

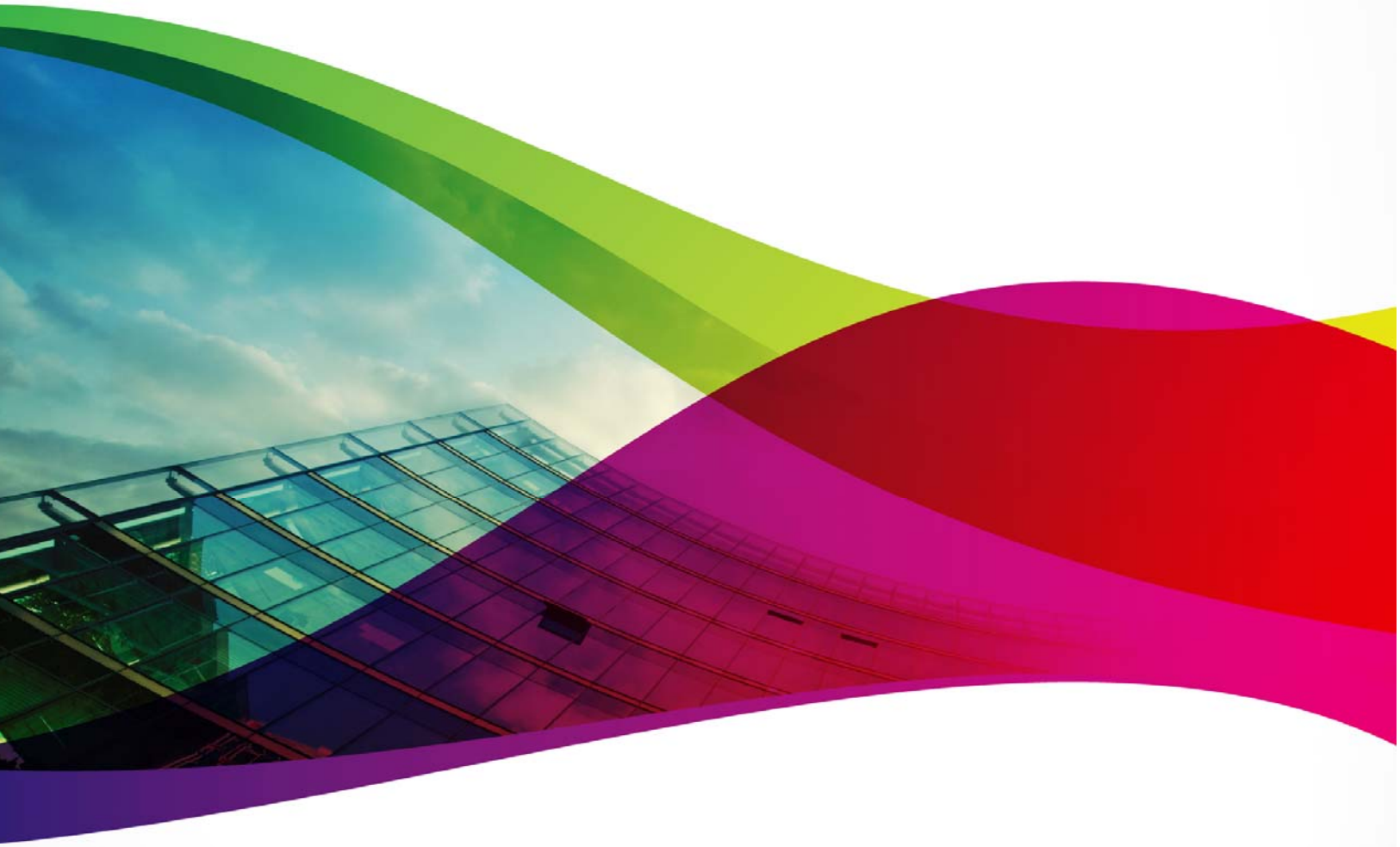


Table of Contents

Importance of Cloud Security in Cloud Environments

Many organizations are looking to the cloud for increasing computational capacity or lowering costs of ownership. While the security issues facing a traditional corporate network are well understood, the challenges of using the cloud are more complex.

Cloud providers spend a great deal of time, effort, and money to ensure that their infrastructures are secure and employ best practices for network design. Industry-standard certifications for cloud datacenters show that physical security, network security, and operating practices can support the stringent requirements of any customer wanting to use their services.

However, most cloud providers have a 'Shared Responsibility Model' – they will provide secure foundations from the physical environment up to the virtualization layer, but the customer is responsible for the security of the operating system and applications. This usually includes ensuring that operating system patches are installed, any applications running in the environment are secure, and items such as firewalls that grant access to the cloud resources are configured correctly. Cloud providers also recommend that customers install appropriate anti-virus and host monitoring software to protect the systems from attack, along with any additional security solutions to help meet key business requirements, such as regulatory compliance issues.

To help meet these requirements, Trend Micro has created the Trend Ready program, to validate that Trend Micro Deep Security and Trend Micro SecureCloud will operate correctly within the Service Provider's cloud environment.

Trend Micro Deep Security

Trend Micro Deep Security provides software-based integrated security and compliance for business systems operating in standalone, virtual, and cloud environments. Deep Security provides core security controls with a unique approach that economically solves the toughest security challenges, including:

- **Virtual Patching**: Discovers host vulnerabilities and recommends rules to shield applications and systems with advanced deep packet inspection technology.
- **Firewall**: An enterprise-grade, bi-directional and stateful firewall enables network segmentation. Deep Security includes centralized management of server firewall policy, and pre-defined templates for common types of enterprise servers.
- **Web Application Protection**: Protects web applications against sophisticated attacks such as SQL injection, cross-site scripting, and more.
- **Antivirus Protection**: Provides lightweight malware protection without compromising system performance.
- **Integrity Monitoring**: Detects and reports malicious and unexpected changes to both physical servers and virtual machines for critical OS and application files, including data files, directories, log files, registry keys and values.
- **Application Control**: Application control rules provide visibility and control over applications accessing the network. Rules can also identify malicious software activity.
- **Logs and Log Inspection**: Analyzes OS and application logs to identify important security events, generates alerts, and optionally forwards to SIEM systems.
- **Virtualization Compliance**: Virtual machine isolation and hardening protects and isolates applications from other VMs executing on the same physical hardware.

Trend Micro Deep Security is available in conjunction with selected Trend Ready cloud service providers as a verified security solution and has been tested within their cloud environments. Deep Security offers security agents for a variety of different platforms, including Microsoft Windows, RedHat and SuSE Linux distributions.

Trend Micro SecureCloud

Trend Micro SecureCloud is designed to encrypt and protect data in public, private, and hybrid clouds while also securing data stored in physical and virtual servers. Easy-to-use, policy-based key management authenticates the identity and integrity of servers requesting encryption keys and controls when and where secure data can be accessed. The Key Management and key generation is abstracted from the cloud service provider to provide separation of duties, ensuring only trusted parties can access encrypted volumes. Trend Micro SecureCloud provides these key features:

- **Industry Standard AES Encryption (with a configurable key length)**: Used to encrypt and decrypt information in real time, so data at rest is always protected.
- **Whole Volume Encryption**: Secures all data, metadata and associated structures without impacting applications– all encryption operations are transparent to running applications.
- **Role-Based Administration**: Ensures separation of duties within your organisation.
- **Automated Key Release and Authorisation**: Delivered via SSL from a Trend Micro SaaS portal, it ensures that encryption keys are delivered securely. The key management duty is separated from the service provider's computing environment.
- **Policy-Driven Key Management**: Uses identity and integrity based policy enforcement to ensure that only authorised systems access secure volumes
- **Robust Auditing, Reporting, and Alerting**: Helps to ensure regulatory compliance requirements are met.

Trend Micro SecureCloud is available in conjunction with selected Trend Ready cloud service providers as a verified security solution and has been tested within their cloud environments. SecureCloud offers encryption agents for a variety of different platforms, including Microsoft Windows, Redhat, SuSE, Ubuntu, and CentOS Linux distributions.

Cloud Security ALLIANCE Guidelines

For many years, Trend Micro has been a consistent supporter and collaborator with the Cloud Security Alliance. As a corporate member and co-chair of its Virtualization Working Group, Trend Micro has worked with the CSA in helping influence cloud security initiatives around the world. The Cloud Security Alliance (http://cloudsecurityalliance.org) has a set of guidelines for best practice utilization of the cloud, available for download at: https://cloudsecurityalliance.org/research/security-guidance/ (registration required). The guidelines are categorized into thirteen 'domains', which highlight areas of concern for an organization wishing to use cloud services. For each of these domains, here is a brief outline of how Trend Micro solutions can help:

CSA Guidelines v3	Compliant?	How Trend Micro and Trend Ready Cloud Service Providers Can Help	Recommended Solutions
Section IIa. Governance Domains			
Governance and Enterprise Risk Management	Yes	Provide full audit logs/activity monitoring in your cloud computing or traditional environment and provide risk/vulnerability assessment for risk management information.	Trend Micro Deep Security
Legal and Electronic Discovery	Yes	Enable Service Providers to run different service models for private or public cloud.	Trend Micro SecureCloud
Compliance and Audit	Yes	Trend cloud security products are ISO 27001/20000, Common Criteria and Security + certified. Key Management is provided as a hosted solution from Trend Micro to ensure encryption keys are not held within the cloud infrastructure to ensure separation of duties.	Trend Micro SecureCloud Trend Micro Deep Security
Information Management and Data Security	Yes	Offer a cloud-based data security architecture to protect data in transition for internal (private cloud) or external (public cloud).	Trend Micro SecureCloud
Portability and Interoperability	Yes	Protect portable data to help minimize the business impact and reduce risk management when changing cloud providers in the future. Enable easy operation and quick deployment to increase the efficiency of service, and aid the IT department in maintaining a consistent security policy while changing environments.	Trend Micro Deep Security Trend Micro SecureCloud
Section IIb. Operational Domains			
Traditional Security, Business Continuity, and Disaster Recovery	Yes	The Trend Micro cloud service provides cross-site redundancy and high availability to avoid business impacts due to a single point of failure.	Trend Micro SecureCloud
Incident Response, Notification, and Remediation	Yes	Monitor systems for attack or vulnerability through Deep Packet Inspection, Integrity Monitoring, and Log Inspection.	Trend Micro Deep Security
Application Security	Yes	Provides trusted data volumes for virtualized and cloud machines, helping customers move their applications to a cloud environment.	Trend Micro SecureCloud

CSA Guidelines v3	Compliant?	How Trend Micro and Trend Ready Cloud Service Providers Can Help	Recommended Solutions
Encryption and Key Management	Yes	Provides volume encryption and key management using AES to protect applications running in the cloud.	Trend Micro SecureCloud
Identity and Access Management	Yes	Provides integrated firewall functions (such as Access Controls, Port, IP, Protocol, and frame type) as well as policy based checking (identity and integrity) to avoid unauthorized access to protected systems.	Trend Micro Deep Security Trend Micro SecureCloud
Virtualization	Yes	Protects hosts and VMs with Host Intrusion Detection and Prevention features, while avoiding resource contention within the virtualization environment.	Trend Micro Deep Security

Implementation Model

Deep Security comprises three major components: The Deep Security Manager, Deep Security Agents and a backend database.

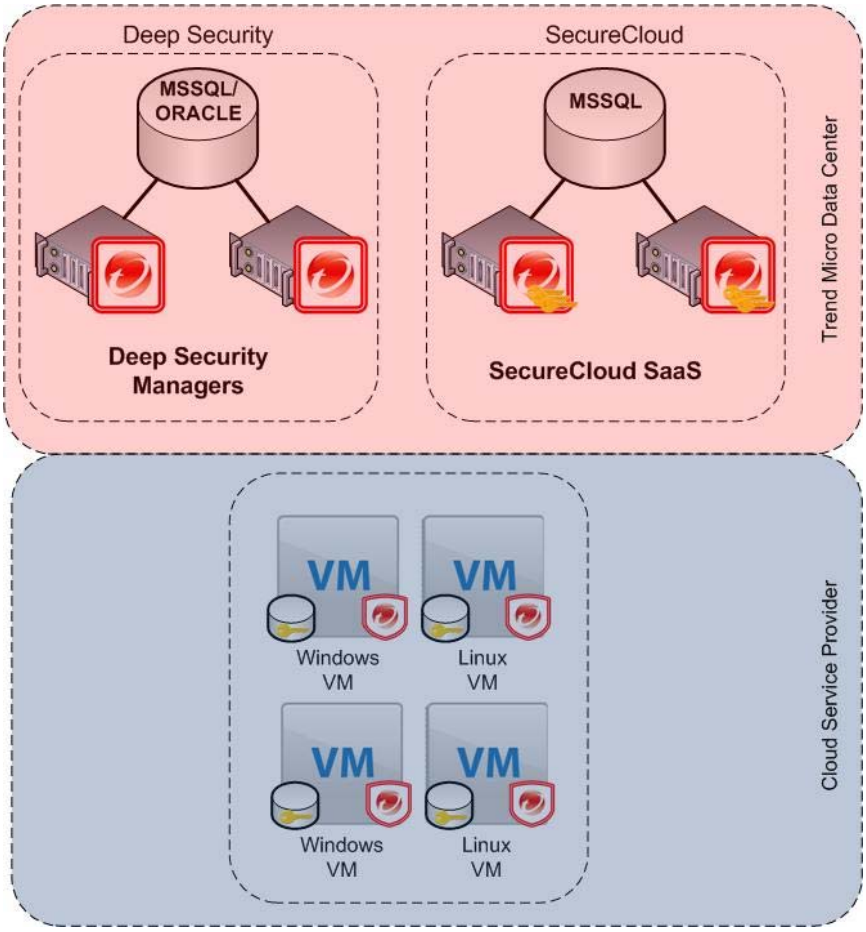
- **Deep Security Agents (DSA)**: This component is the enforcement point for all protection functionality on a host computer. The nature of that protection depends on the rules and security settings that each DSA receives from the Deep Security Manager.
- **Deep Security Manager (DSM)**: This is the management component of the system and is responsible for sending rules and security settings to the Deep Security Agents. The DSM is controlled using the DSM management console. It uses its database and other network services required for proper operation (e.g., Active Directory, ESX servers, security center, etc.)
- **Database**: The database contains all persistent information that DSM needs to operate. This includes configuration details and log information for each individual protected host, and other records required for DSM operation.

To perform the validation of Deep Security within the Cloud Service Provider's environment, DSAs will be installed on a set of evaluation virtual machines, and a DSM hosted in Trend Micro's data center will be used to activate and push policy to these DSAs.

SecureCloud comprises major components: the Trend Micro SecureCloud SaaS service and SecureCloud Agents.

- **SecureCloud SaaS:** Trend Micro hosts the SecureCloud Management Server with multi-tenant capability. There is no enterprise console option for SecureCloud SaaS. The Management Server hosts the key approval process, log collection, and reporting.
- **The SecureCloud Agent:** This component communicates with the Cloud Service Provider (CSP) to retrieve the metadata (location, IP-address, MAC-address, etc.) and with the Key Management Server (KMS) to retrieve encryption keys. To perform the validation of SecureCloud within a Trend Ready Cloud Service Provider's environment, the Trend Micro SaaS Key Management Server was used; however, other deployment options are available. Please refer to the SecureCloud product documentation for additional information.

Reference Architecture



Validation Methodology

To verify Deep Security in the Trend Ready Cloud Service Provider's environment, the following tasks are carried out:

1. Install the Deep Security Agent on a supported platform offered by the cloud provider.
   If the provider is offering Deep Security Agentless protection, no agent installation is required, but testing is still carried out to verify functionality.
2. Activate the Deep Security Agent(s).
3. Assign a Security Profile enabled for all protection modules (Firewall, Deep Packet Inspection, Log Inspection, Integrity Monitoring, Anti-Malware).
4. Carry out per-module validation testing.
5. De-activate and uninstall the Deep Security Agent(s).

To verify SecureCloud in the Trend Ready Cloud Service Provider's environment, the following tasks are carried out:

1. Install the SecureCloud Agent on a supported platform offered by the cloud provider.
2. Execute the configuration utility.
3. Create and attach a new volume for encrypted data.
4. Configure and encrypt a new volume.
5. Create a sample dataset on the encrypted volume.
6. Revoke key access and ensure the encrypted data is inaccessible.

Validation Results

In order for the validation methodology to be considered successful, the following tests need to be passed:

- All Deep Security modules tested successfully in the Trend Ready Cloud Service Provider's environment.
- Firewall and Deep Packet Inspection rules were assigned to the network interfaces and triggered successfully.
- Integrity Monitoring rules were enabled and changes to critical system files were properly identified.
- The Log Inspection functionality was enabled and triggered on simulated security events in the system logs.
- Anti-Malware capabilities were enabled and properly detected the presence of a test malware sample.
- SecureCloud functionality was successfully verified by adding and encrypting a new volume and ensuring that all encrypted data was accessibly only after valid integrity checks were performed.

Key Contacts /More Information

About Trend Micro

Trend Micro Incorporated (TYO: 4704;TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge – from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

Additional information about Trend Micro Incorporated and the products and services are available at trendmicro.com. Or follow our news on Twitter at @TrendMicro.

About the CSA

The Cloud Security Alliance is a not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. For further information, visit them at www.cloudsecurityalliance.org, and follow them on Twitter @cloudsa.

Trend Micro is the founding sponsor of Cloud Security Alliance Asia Pacific, and Ken Low of Trend Micro currently holds the CSA Asia Pacific Council Chairman's role.

TREND MICRO™
Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site: www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax:+1408.257.2003

www.trendmicro.com.