

Trend Micro

SecureCloud™

Securing and Controlling Sensitive Data in the Cloud

More companies are turning to cloud computing and virtualization to provide rapid provisioning, agility, and cost savings. However, these benefits also introduce privacy and security risks—businesses may not always know where their data is or who can access it. Trend Micro SecureCloud™ provides distinctive data protection for cloud and virtual environments using **encryption with policy-based key management and unique server validation**. This protection safely and easily secures sensitive data stored with leading cloud service providers, including Amazon EC2, Dell, Eucalyptus, and NTT America, as well as VMware vCloud and any virtual environment¹.

SecureCloud provides a patent-pending, key management system that enables you to set policies that determine where and when encrypted data can be accessed. In addition, server validation applies identity and integrity rules when servers request access to secure storage volumes. SecureCloud's simple approach safely delivers encryption keys to valid devices without the need to deploy an entire file system and management infrastructure.

With SecureCloud, you can protect sensitive information in cloud and virtual environments from theft, unauthorized exposure, or unapproved geographic migration to other data centers. This protection helps support internal governance and **ensure compliance with regulations like HIPAA, HITECH, Sarbanes-Oxley, GLB and PCI DSS**. SecureCloud also features FIPS 140-2 certification to support government agencies and companies that mandate high security standards.

The SecureCloud key management and data encryption solution is available as Software as a Service (SaaS) or as a software application. By giving your business control of its own keys, SecureCloud gives you the freedom to encrypt data in virtual data centers or in the cloud, and even to move between cloud vendors without being tied to any one provider's encryption system.

KEY FEATURES

Advanced Security Techniques

- Features FIPS 140-2 certification and FIPS approved AES encryption
- Encrypts and decrypts information in real time, so data at rest is always protected
- Applies whole volume encryption to secure all data, metadata, and associated structures without impacting application functionality

Access and Authentication Controls

- Employs role-based management to help ensure proper separation of duties
- Automates key release and virtual machine authorization for rapid operations or requires manual approval for increased security
- Offers cloud provider credential rotation²

Policy-driven Key Management

- Uses identity- and integrity-based policy enforcement to ensure only authorized virtual machines receive keys and access secure volumes
- Integrates with Deep Security Manager to further validate the environment security posture
- Enables the use of policies to determine when and where information is accessed

Robust Auditing, Reporting, and Alerting

- Logs actions in the management console for audit purposes
- Provides detailed reporting and alerting features with incident-based and interval-based notifications

SAAS OR SOFTWARE APPLICATION

Protection Points

- Private Cloud
- Public Cloud (Infrastructure-as-a-Service)
- Virtual Environments

Threat Protection

- Data Privacy
- Regulatory Compliance
- Secure Storage Recycling

KEY BENEFITS

Infrastructure

- Provides safe use of IaaS, leveraging the agility and cost savings of the public cloud
- Segregates and protects sensitive information in private clouds and virtual environments

Security

- Enhances data security and control by remotely managing cipher keys
- Promotes safe storage recycling by rendering any data remnants indecipherable
- Facilitates compliance and supports internal governance

Choice

- Allows businesses to choose when and where information is accessed
- Avoids vendor lock-in with customer key ownership

¹ Can run on any virtual environment running in a supported operating system.

² Limited to Amazon Web Services

PLATFORMS SUPPORTED

Infrastructure Providers	Host Operating Systems
<ul style="list-style-type: none"> • Amazon EC2 • Eucalyptus • vCloud • RightScale • TCloud • VMware ESX and vSphere 	<ul style="list-style-type: none"> • Windows 7 • Windows Server 2003 R2 SP2 (32/64-bit) • Windows Server 2008 R2 SP2 (32/64-bit) • Windows Server 2008 SP2 (32/64-bit) • CentOS 5.6, 6.0 (32/64-bit) • Red Hat Enterprise Linux 5, 6 (32/64-bit) • Ubuntu 10.10, 11.04 (32/64-bit) • SUSE OpenSuSe 11.1, 11.4 (32/64-bit)

MINIMUM SYSTEM REQUIREMENTS

SecureCloud offers key management as a Trend Micro SaaS solution or as a software application managed within the user's data center.

SaaS Deployment
<ul style="list-style-type: none"> • Internet connection • Web browser
Software Application Management Server Deployment
Hardware Requirements: <ul style="list-style-type: none"> • CPU: One virtual-core processor • Memory: 768MB • Hard disk space: 85MB to install SecureCloud Management Server
Databases Supported: <ul style="list-style-type: none"> • Microsoft SQL 2008 Server R2 Express with Advanced Services • Microsoft SQL 2008 Server R2 Enterprise with Reporting Services
Management Server Supported operating systems: <ul style="list-style-type: none"> • Windows Server 2003 R2 SP2 32-bit • Windows Server 2008 SP2 32-bit • Windows Server 2008 R2 64-bit • Windows Server 2003 Active Directory (used for Active Directory) • Windows Server 2008 Active Directory (used for Active Directory)

COMPLEMENTARY PRODUCTS

Physical, Virtual, and Cloud Server Security

- **Trend Micro Deep Security** works in combination with Trend Micro SecureCloud to provide advanced protection for servers in the dynamic data center, whether physical, virtual, or in the cloud. Deep Security combines anti-malware, intrusion detection and prevention, firewall, integrity monitoring and log inspection capabilities in a single, centrally managed software agent. To maximize both protection and virtual machine densities, you can also deploy agentless anti-malware, intrusion defense, and integrity monitoring.

[Learn more >](#)

Cloud Protection Module enables SecureCloud to query Deep Security Manager to gather information about the security status of servers before they are accessed. This integration helps you increase your overall security posture by building policies around this new information and enhancing the rules that govern when and to which servers keys are released.



©2012 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo 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. [DS01_SecureCloud2_120305US]

www.trendmicro.com