More and more, companies are turning to cloud computing and virtualization to provide rapid provisioning, agility, and cost savings. However, along with these benefits also come data privacy and security concerns. Organizations are used to having physical control over where their sensitive information is stored and how it is accessed. When moving to the cloud, organizations can implement additional data protection, like encryption, to provide the confidence that their data can’t be accessed without authorization.

**Trend Micro SecureCloud™** addresses the issue of data protection for cloud and virtual environments with full-disk encryption and a policy-based key management and unique server validation solution. This safely and easily secures sensitive data stored with leading cloud service providers such as Microsoft Azure, Amazon Web Services, and VMware vCloud Air, or in virtual environments like VMware vSphere.

SecureCloud provides a policy-driven key management system so you determine where and when encrypted data can be accessed. In addition, identity and integrity rules are applied when servers request access to secure storage volumes. SecureCloud’s simple approach to data protection 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 from theft, unauthorized exposure, or unapproved geographic migration to other data centers. This protection helps support internal governance and achieve compliance with regulations like HIPAA, HITECH, Sarbanes-Oxley, and PCI DSS. SecureCloud has AES-256 block-level encryption and is FIPS 140-2 certified to support U.S. government agencies.

By giving you control of your own keys, SecureCloud gives you the freedom to control your encrypted data in virtual data centers or the cloud, and even to move between cloud vendors without being tied to a provider’s encryption system. SecureCloud is available as a service or as software.

**KEY BENEFITS**

**Lets you govern your own keys**
- You control your keys to ensure only authorized parties can see/access data.
- Avoid vendor lock-in by managing your own keys, allowing you to switch providers with no encryption issues.

**Encrypts both primary (boot) and secondary volumes**
- Includes full data encryption, transparent to the database servers and other applications, with minimal overhead.

**Convenient management and key release**
- Central key management with policy-based key release automates when and where data may be accessed.
- Automatically authenticates the identity and integrity of servers requesting keys.

**Assures data destruction**
- Ensures that any data in the cloud is not accessible even after instances are decommissioned.

---

* Primary volume encryption is only available on select operating systems.
**KEY FEATURES**

**Policy-driven Key Management**
- Uses identity- and integrity-based policy enforcement to control keys and data encryption.
- Enables the use of policies to determine when and where information is accessed.

**Key Management Interoperability Protocol (KMIP) Support (on-premises only)**
- Establishes a single, comprehensive protocol for the communication between key management systems, letting admins continue to use existing key management solutions.
- Validates the identity and integrity of the environment before releasing the encryption keys.

**Advanced Security Techniques**
- FIPS 140-2 certified with 256-bit AES encryption.
- Encrypts and decrypts information in real time, so data at rest is always protected.
- Encrypts whole volume to secure all data, metadata, and associated structures without impacting functionality.

**Access and Authentication Controls**
- Employs role-based management to ensure proper separation of duties.
- Automates key release and virtual machine authorization for rapid operations.
- Provides credential rotation for AWS instances.

**Robust Auditing, Reporting, and Alerting**
- Logs actions in the management console for audit purposes.
- Provides detailed reporting and alerting features with incident- or interval-based notifications.

**SECURECLOUD WORKS ON**

<table>
<thead>
<tr>
<th>Infrastructure Providers</th>
<th>Host Operating Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Microsoft Azure Virtual Machines</td>
<td>• Windows 7, 8, 8.1</td>
</tr>
<tr>
<td>• Amazon Web Services EC2 and VPC</td>
<td>• Windows Server 2003-2012 R2</td>
</tr>
<tr>
<td>• VMware vCloud Air Virtual Machines</td>
<td>• CentOS 5.9-5.10, 6.4-6.5, 7.0</td>
</tr>
<tr>
<td>• VMware vSphere Virtual Machines</td>
<td>• Oracle Linux 6.4</td>
</tr>
<tr>
<td></td>
<td>• Red Hat Enterprise Linux 5.9-5.10, 6.4-6.5, 7.0</td>
</tr>
<tr>
<td></td>
<td>• Ubuntu 10.04, 12.04, 14.04</td>
</tr>
<tr>
<td></td>
<td>• SUSE Linux Enterprise 11 SP2, 11 SP3</td>
</tr>
<tr>
<td></td>
<td>• AWS Linux</td>
</tr>
</tbody>
</table>

See installation guide for information on which operating systems support which infrastructures for data and boot encryption

http://docs.trendmicro.com/all/ent/sc/v3.7/en-us/sc_3.7_ig.pdf

Supports 32/64-bit for all of above