

# Trend Micro™ Cloud Protection

## Securing Your Unique Cloud Journey

As you look to the cloud for increased IT agility and cost savings, you'll need to be diligent about ensuring the safety of your cloud servers, applications, and data. Often businesses use traditional physical server security in their virtual and cloud infrastructure, but this can cause resource and management issues and expose you to business disruption and data breach. As virtualization is the foundation of the cloud, you need virtualization-aware security to help you maximize both protection and performance in your cloud environment.

However, the cloud also introduces unique risks with its shared resource infrastructure—endangering the security and privacy of cloud systems, applications, and data. That's why you need to provide adaptive protection through a single server security platform that has been designed specifically to protect systems and applications in cloud environments, as well as virtual and physical servers. The platform should integrate multiple security technologies, such as anti-malware, firewall, intrusion prevention, web application protection, and integrity monitoring. And this should be combined with encryption and policy-based key management to protect your data stored in the cloud. A unified approach to cloud protection will provide flexible, cost effective security for your servers, applications, and data in private, public and hybrid clouds.

### Protecting Private Clouds

Private clouds are based on dedicated hardware either located in your data center or outsourced to a third party. Automated provisioning is added to a virtualized environment to create a private cloud portal that provides on-demand, self-service IT resources. But security challenges such as shared internal resources, mobile data, and VM sprawl can limit the success of private clouds.

Your security strategy for private clouds should start with agent-less security—ideal for virtual infrastructures and private clouds. With control over the hypervisor, you can deploy a dedicated security virtual appliance on each host that can provide security services such as anti-malware, intrusion prevention, and integrity monitoring to all guest virtual machines. This tamperproof approach strengthens protection with the added advantages of a virtually zero footprint, increased consolidation ratios, and significant improvements in security administration.

Encryption is also important for private clouds, especially if regulatory compliance or internal governance mandates that certain data be kept confidential between particular internal departments. And if the private cloud infrastructure is outsourced to a third party, encryption ensures that sensitive data remains confidential from the service provider.

### Protecting Public Clouds

With the public cloud, service providers offer computer resources through online services. This allows you to quickly configure, deploy, or expand your services online and only pay for the resources you use. The public cloud provides better cost savings, but the shared infrastructure also introduces increased risk and limits visibility.





Advanced application security technologies such as intrusion prevention and integrity monitoring become even more critical in this environment. Because you lack control of the hypervisor in public clouds, agent-based security will help you create self-defending VMs in the multi-tenant environment.

Data stored in the public cloud must be encrypted to prevent access by service provider staff and rogue servers. Encryption also ensures that any data remnants from recycled storage volumes are made unreadable if accessed by an unauthorized source. With effective encryption, even heavily regulated businesses can leverage the economies of the public cloud.

### Protecting Hybrid Clouds

Hybrid clouds combine the onsite control of a private cloud with the scalability of the public cloud. This allows you to keep more mission-critical data and applications in house while leveraging the cost savings of the public cloud for storage and temporary computing capacity needs.

Security for hybrid clouds must span both the private and public cloud infrastructures. To keep data and applications safe throughout the hybrid cloud, you'll need self-defending VMs using agent-less security for the private cloud as well as agent-based security for the public cloud. And encryption can be a great equalizer for data that is stored in either a private or public cloud.

### Comprehensive, Adaptive, Efficient Cloud Protection

**Trend Micro Deep Security** delivers protection across physical, virtual and cloud servers—securing systems and applications in private, public, and hybrid clouds with integrated technologies:

- Anti-malware
- Integrity monitoring
- Bidirectional stateful firewall
- Intrusion detection and prevention
- Web application protection
- Log inspection
- Encryption through integration with Trend Micro SecureCloud

Deep Security integrates with VMware APIs to provide the industry's first agent-less, virtualization-aware security for private clouds. Agent-based protection is also available to secure VMs in public cloud environments, as well as physical servers and non-VMware virtual machines.

**Trend Micro SecureCloud** provides encryption with simple, patent-pending, policy-based key management designed to protect data in various cloud environments as well as physical and virtual infrastructures. Through integration with Deep Security, SecureCloud validates that servers requesting encryption keys have up-to-date protection from Deep Security before keys are released. SecureCloud enables you to:

- Control when and where data is accessed with policy-based key management
- Conduct server validation with identity- and integrity-based checks
- Deploy as a hosted service or as an on-premise software application with customer key ownership
- Encrypt data in virtual data centers or in the cloud, and even move data between cloud vendors

Together, Deep Security and SecureCloud provide a holistic approach to cloud protection to mitigate the risks of data breach, theft, and data motility. Deploying protection for systems, applications, and data that travels between physical, virtual, and private, public, and hybrid cloud servers provides better protection, less administrative complexity, and increased performance. As a recognized leader in virtualization and server security, Trend Micro offers proven solutions that will help you accelerate your virtualization and cloud ROI.

