


A background image showing a laptop on a desk with a speedometer overlay, suggesting performance and security.

# Total Cloud Protection

Data Center and Cloud Security 

 Security for Your  
Unique Cloud  
Infrastructure

*A Trend Micro White Paper | August 2011*

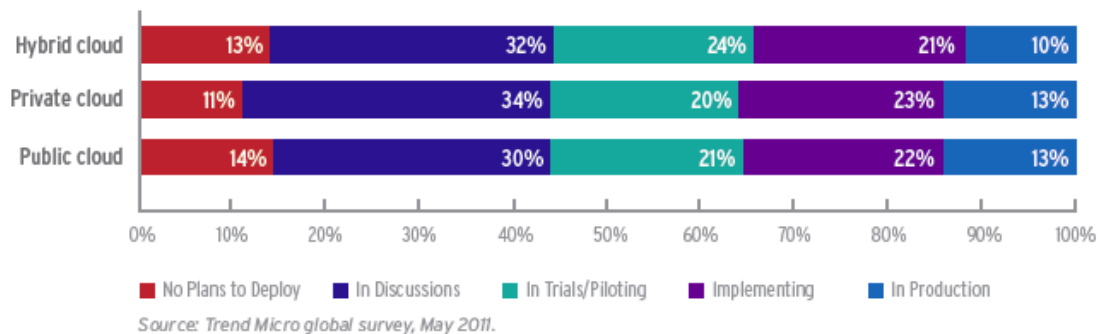


# SECURITY FOR YOUR UNIQUE CLOUD INFRASTRUCTURE

## I. INTRODUCTION

Many businesses are looking to the cloud for increased IT agility and cost savings. Yet the types of clouds that are deployed vary with business needs. In a recent study by Trend Micro, the results showed that there is almost an even distribution across private, public, and hybrid cloud deployments. For clouds already in production, 13 percent of business had deployed a private cloud; 13 percent had deployed a public cloud; and 10 percent had deployed a hybrid cloud. Another 21-23 percent are in the midst of implementing each of the cloud models, and 30-34 percent are trialing or piloting a cloud.

### Business Cloud Deployment by Cloud Model



In addition to showing a relatively even distribution of adoption across the different cloud models, these results also show that actual clouds in production will increase four fold in the near future as clouds in the midst of implementation and in trial go into production.

As businesses develop their cloud infrastructure, security must be part of the groundwork to ensure that cloud servers, applications, and data remain secure in a cloud environment. Often businesses use traditional physical server security in virtual and cloud infrastructure. But this can cause resource contention issues, increase management complexity, reduce virtual machine (VM) densities, and lower expected return on investment (ROI).

Virtualization is the foundation of cloud infrastructure, requiring virtualization-aware security to maximize protection and performance. However, moving applications and data into the cloud also introduces unique risks—in all three cloud models: private, public, and hybrid. A comprehensive, adaptive, and efficient approach to cloud protection is needed regardless of which cloud model businesses deploy or how their cloud computing needs evolve.

This paper discusses each of the three cloud models, their unique security risks, and the security solutions that best address those risks. With the right security, companies can safely implement any of the cloud models, even if those companies are subject to strict data privacy regulations. When selecting a cloud model, businesses should consider how it will impact their business objectives, security and compliance requirements, and IT resources.



# SECURITY FOR YOUR UNIQUE CLOUD INFRASTRUCTURE

## II. PRIVATE CLOUDS

Private clouds are based on dedicated hardware that is either located in the businesses data center or outsourced to a third party. The underlying infrastructure is a virtualization environment and IT resources are provided through an on-demand, self-service portal. The automated provisioning is what converts the virtualization infrastructure into a “cloud.” Different departments can gain access to IT resources through an online catalog and bill-back functions can bill individual departments for their IT resource consumption.

The automation of a private cloud can provide companies with IT resource agility, allowing different departments to gain access to computing resources quickly, as needed—no longer having to submit a request to IT staff to meet these needs. However, security designed for a cloud environment is integral to ensuring safe cloud computing. With self provisioning, private clouds can quickly pool resources and VMs can be moved to optimize resources. With shared resources, mobile data, and possible VM sprawl, security and visibility are critical to mitigate privacy and compliance risks.

With private clouds, there are three elements that should be combined for comprehensive security:

- VM-level security
- Agent-less security to maximize resources
- Encryption with policy-based key management

### ***VM-Level Security***

Virtualization serves as the foundation to cloud computing, allowing businesses to make the best use of resources. When extending virtualization into a cloud infrastructure, the security used on the virtual servers can also be used in a cloud environment.

Private clouds make it easy to provision new virtual machines. And even different departments can have resources that are all housed on the same host physical server. This can create a mixed-trust level environment—with applications and data of differing trust levels on a single host server. Providing security at the network level, such as network firewalls or an intrusion prevention system (IPS), will not protect the individual guest virtual machines from inter-VM attacks. Another security approach might be to route inter-VM communications to a separate physical security appliance—but requiring communications to be routed off box through the separate appliance creates performance and security lags. In addition, compliance regulations may require that certain data stay isolated from other VMs and retain restricted access. To address these issues, security must be provided at the VM level.

VM-level protection should integrate multiple security technologies including, intrusion prevention, firewall, anti-malware, web application protection, log inspection, and integrity monitoring. Even as VMs are moved or reconfigured to make the best use of resources, these protections can travel with the VM to ensure security and will better equip the VM to protect itself as it moves into riskier environments.



## SECURITY FOR YOUR UNIQUE CLOUD INFRASTRUCTURE

### ***Agent-less Security to Maximize Resources***

Traditional physical security on virtual servers saps resources because it is not virtualization aware. When conducting periodic security scans, physical security will initiate a simultaneous scan of all virtual machines, which significantly degrades host resources and performance. Some traditional physical security solutions recommend randomization or grouping in virtual environments, but these do not solve the problem. Randomization does not help to avoid times of high system usage and requires that a long period of time be reserved for the full scan cycle. Grouping does not allow for the mobile nature of virtualization, requiring reconfiguration when virtual machines are migrated or cloned. Virtualization-aware technology is needed to minimize resource usage and increase virtual machine densities.

Agent-less security in a virtualization-aware solution optimizes virtualization and cloud performance. Because private clouds are based on dedicated hardware, businesses have control of the underlying hypervisors. Agent-less security—such as agent-less antivirus and agent-less file integrity monitoring—uses a dedicated virtual machine that integrates with hypervisor APIs to conduct security scanning. The security virtual appliance accesses a small footprint driver in each guest VM to coordinate staggered updates and scans. Resource-intensive operations, such as full system scans, are run from the separate virtual appliance, maximizing host resources.

Using a dedicated security virtual appliance also ensures that VMs always have up-to-date security. Guest VMs are secure when dormant and receive the latest pattern file updates when activated. In addition, agent-less security reduces management complexity because there are no agents to configure or update.

### ***Encryption with Policy-based Key Management***

Encryption is generally understood to be a security best practice for sensitive data. In the inter-departmental shared resource environment of a private cloud, this becomes more important. Often data must be kept confidential even between particular departments, whether it is due to regulatory compliance requirements or internal governance for data such as customer information, employee records, or intellectual property. And if the private cloud infrastructure is outsourced to a third party, sensitive data must also be kept confidential from the service provider.

Although industry-standard encryption is essential, a cloud encryption solution must go beyond simply encrypting the data. Policy-based key management is needed to control when and where data is accessed. In addition, server identity and integrity checks are needed to ensure that only authorized servers can access encrypted data and that these servers have up-to-date security prior to access.

Another important component to a cloud encryption solution is that the customer must retain key ownership. If the private cloud is outsourced, this maintains a separation of duties between the business and the service provider. Customer key ownership also allows companies to move data between clouds and keep control of their encryption service.



## SECURITY FOR YOUR UNIQUE CLOUD INFRASTRUCTURE

### III. PUBLIC CLOUDS

With the public cloud, service providers offer computer resources through online services, enabling businesses to quickly configure, deploy, or expand services online and only pay for the resources they use. The public cloud provides better cost savings because of the shared, multi-tenant architecture which makes better use of resources and reduces vendor costs. These cost savings make public clouds especially popular for storage. Companies also use public clouds for projects requiring temporary or varying compute needs because of the pay-per-use approach. They can use the public cloud instead of building out internal infrastructure for only partial or temporary usage. But the shared infrastructure also introduces increased risk and more limited visibility.

With Software as a Service (SaaS) and Platform as a Service (PaaS) public clouds, the service provider is responsible for most of the security. But with Infrastructure as a Service (IaaS), the customer is responsible for securing their virtual machines deployed in the public cloud. In the multitenant environment of IaaS public clouds, businesses do not know what type of applications or data are housed next to their computing resources. In a private cloud, cybercriminals would simply need to gain access to a VM on a host machine to conduct an inter-VM attack. However, in the public cloud, cybercriminals have it even easier—they can purchase their own VMs within the shared infrastructure and use these to attack other guest VMs or even try to compromise the hypervisor which controls access to guest VMs.

Visibility can also be an issue. Companies may not be able to track who has accessed their data. For example, has the service provider viewed their data? Or have rogue servers accessed their storage volumes? And perhaps cybercriminals have stolen or compromised data through inter-VM attacks.

Data motility is another concern in the public cloud. Service providers move customers' data to make the best use of resources. This means that the customer may be unaware of where specifically their data is being stored at any given time. Also, to ensure high availability, service providers may replicate data across multiple data centers. Or storage administrators might make storage volume snapshots for disaster recovery purposes. This goes beyond the experience of *data mobility*, the ability to move their data, to *data motility*, the experience of spontaneous data movement uncontrolled by the data owner.

Companies benefit when service providers move data to optimize resource usage because this lowers costs. However, data is often moved without customer knowledge or visibility. When data is moved, prior data storage volumes should be shredded. Yet sometimes data remnants remain, which can expose data to unauthorized sources. And businesses may be oblivious to this unpermitted access.

Companies need a combination of security and visibility to ensure their cloud applications and data remain secure and they can meet their regulatory and internal compliance requirements. Elements for public cloud security include the following:

- Agent-based, self-defending VM security
- Encryption with policy-based key management



## SECURITY FOR YOUR UNIQUE CLOUD INFRASTRUCTURE

### ***Agent-based, Self-defending VM Security***

Without hypervisor control, agent-based security creates self-defending VMs in the multi-tenant environment of the public cloud. Self-defending VMs are needed to prevent inter-VM attacks and maintain VM isolation. In a private cloud, agent-less security optimizes resources. However, in a public cloud the service provider is able to optimize resource usage for its customers with economies of scale as well as ease of data motility in the public cloud virtual environment. So, instead, agent-based, self-defending VMs are needed to protect applications and data regardless of what is housed next to the company computing resources or where the data may be moved.

A similar mix of advanced security technologies as mentioned in the private cloud section—intrusion prevention, firewall, anti-malware, web application protection, log inspection, and integrity monitoring—is needed in the public cloud. Due to the prevailing levels of risk, these protections are even more critical. The integrated server security platform agent travels with the VMs wherever they are stored in the shared IaaS public cloud environment always maintaining an umbrella of protection over the VM.

### ***Encryption with Policy-based Key Management***

Data stored in the public cloud must also be encrypted to prevent access by unauthorized individuals and rogue servers. Also any data remnants from recycled storage volumes would be made unreadable if accessed by an unauthorized source.

But again, the solution must go beyond industry-standard encryption to include policy-based key management and server validation. Data motility in the public cloud can make the actual location of data unpredictable. But granular policy control can specify when and where data can be retrieved and supports data privacy regulations which require that data only be accessed in particular geographic regions.

Server validation can prevent access by rogue servers using identity-based checks prior to releasing keys. Integrity-based checks also ensure that server security is up to date. And a public cloud encryption solution needs to provide reporting and auditing to show who has accessed the company's data. With encryption, even heavily regulated businesses can leverage the economies of the public cloud.

Customer key ownership is important here as well. This maintains a separation of duties with the service provider, but also avoids vendor lock in. Companies retain the freedom to bring their data back in house or switch between service providers without having to change encryption solutions.



## SECURITY FOR YOUR UNIQUE CLOUD INFRASTRUCTURE

### IV. HYBRID CLOUDS

Hybrid clouds combine the onsite control of a private cloud with the scalability of the public cloud. Businesses can keep more mission-critical data and applications in house while leveraging the cost savings of the public cloud for storage and temporary compute capacity needs. Some technologies even help organizations seamlessly move resources between private and public clouds as needed.

Generally a hybrid cloud is considered an on-going deployment across both a private and public cloud, but organizations can also use “cloudbursting.” This happens when a private cloud does not have sufficient resources and the company “bursts” out into a public cloud to cover temporary resource needs.

Although hybrid clouds allow companies to decide whether to store particular types of application and data in private or public clouds, this creates the largest potential attack surface as resources span both cloud models. Security for hybrid clouds must have flexible deployment options that protect both private and public cloud infrastructures with consolidated management for ease of use. The security elements for a hybrid cloud include the following:

- Agent-less and agent-based VM security
- Encryption with policy-based key management

#### ***Agent-less and Agent-based VM Security***

The ideal hybrid cloud security solution combines both agent-less and agent-based VM security. Agent-less security optimizes resources in the private cloud component and the agent-based security creates self-defending VMs in the public cloud. With both deployment options, data and applications are kept safe throughout the hybrid cloud.

Both agent-less and agent-based security should be integrated in a single platform with consolidated management. A company should be able to manage security for all types of cloud deployments through one console. This allows seamless protection as VMs are moved between private and public clouds, as well as between different service providers.

#### ***Encryption with Policy-based Key Management***

Encryption can be a great equalizer in a hybrid cloud because encrypted data may be stored securely in either a private or public cloud. Businesses can select a cloud deployment based on resources and cost savings rather than on security concerns.

Again, consolidated management and customer key ownership is critical. If a company owns the keys, they can encrypt all public and private components of their hybrid cloud, move data between clouds, and switch service providers as needed. And all components can be managed through one encryption key service, providing visibility into encryption and data access across the entire hybrid cloud.



## SECURITY FOR YOUR UNIQUE CLOUD INFRASTRUCTURE

### V. COMPREHENSIVE, ADAPTIVE, EFFICIENT CLOUD PROTECTION

Trend Micro offers two products that protect across physical, virtual, and cloud servers and data. Not only do these products protect all three of these environments, they are also specifically designed to combat the risks unique to each platform while maximizing performance.

#### *Cloud Server Security*

**Trend Micro Deep Security** provides a single platform for server, application, and data security for virtual desktops and across physical, virtual, and cloud servers—protecting private, public, and hybrid clouds. Businesses can tailor their security with any combination of agent-less and agent-based protection—including anti-malware, firewall, intrusion detection and prevention, web application protection, integrity monitoring, and log inspection as well as encryption and policy-based key management through integration with Trend Micro SecureCloud. The Deep Security platform includes the following modules:

- **Anti-malware Protection** defends against viruses, spyware, Trojans and other malware. This module detects malware in real time and incorporates cleanup capabilities to help remove malicious code and repair any system damage caused by the malware.
- **Firewall Protection** provides a bi-directional stateful firewall with centralized management of server firewall policy and includes pre-defined templates for common enterprise server types.
- **Intrusion Detection and Prevention (IDS/IPS)** shields vulnerabilities in operating systems and enterprise applications until they can be patched. Intrusion detection and prevention helps enterprises achieve timely protection against known and zero-day attacks. Deep Security includes out-of-the-box vulnerability protection for over 100 applications.
- **Web Application Protection** rules defend against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities, and shields these vulnerabilities until code fixes can be completed. Deep Security enables compliance with PCI Requirement 6.6 for the protection of web applications and the data that they process.
- **Application Control** rules provide increased visibility into, and control over, the applications that are accessing the network. These rules can also be used to identify malicious software accessing the network or to reduce the vulnerability exposure of your servers.
- **File Integrity Monitoring** inspects files, systems, and registry for changes. Integrity monitoring of critical operating system and application files (e.g., files, directories, registry keys and values, etc.) is necessary for detecting malicious and unexpected changes that could signal a compromise of virtual and cloud computing resources.



## SECURITY FOR YOUR UNIQUE CLOUD INFRASTRUCTURE

- **Log Inspection** provides visibility into important security events captured in log files. Log inspection rules optimize the identification of important security events buried in multiple log entries from numerous sources. These events can be aggregated and sent to a stand-alone security system or forwarded to a security information and event management (SIEM) system for correlation with other infrastructure events, reporting, and archiving.

To achieve the agent-less deployment option of the above modules, Deep Security tightly leverages and integrates with VMware products and APIs. Deep Security was the first product to integrate with VMware vShield Endpoint APIs for agent-less antimalware and agent-less file integrity monitoring (FIM). This vShield integration enables the offloading of anti-malware and FIM processing to a dedicated, security-hardened virtual machine. And by integrating with VMware VMsafe APIs, Trend Micro offers other agent-less protection, including HIPS, web application protection, application control, and firewall. In virtual and private cloud environments this agent-less security uses the dedicated security virtual machine to eliminate the agents off the guest virtual machines and reduce the resource burden on the underlying host—preserving performance and increasing VM densities. This agent-less approach also reduces administration with no agents to configure or update.

An agent-based option is available for each of the modules as well to allow companies to deploy self-defending VMs in a public cloud environment. Agent-based security also allows the protection to extend to physical servers as well as to virtual desktops while in local mode. The mix of agent-less and agent-based deployment options result in a comprehensive, adaptive, and efficient server security platform. Together the modules in the Deep Security platform protect mission-critical applications and data to prevent data breaches and ensure business continuity across physical, virtual, and cloud environments.

### **Cloud Data Encryption**

**Trend Micro SecureCloud** provides encryption with simple, patent-pending, policy-based key management designed for different cloud environments as well as physical machines and virtual infrastructures. Businesses can safely and easily secure sensitive data stored with leading cloud service providers, including Amazon EC2, Eucalyptus, and vendors delivering VMware vClouds, as well as VMware vSphere virtual environments.

With SecureCloud, businesses can 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. Integration with Deep Security supports the integrity rules, allowing SecureCloud to validate that servers have up-to-date security prior to releasing encryption keys. SecureCloud's simple approach safely delivers encryption keys to valid devices without the need to deploy an entire file system and management infrastructure.

The SecureCloud key management and data encryption solution is available as Software as a Service (SaaS) or as a software application. With customer key ownership, businesses control their own keys. This gives businesses 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.



## SECURITY FOR YOUR UNIQUE CLOUD INFRASTRUCTURE

### ***Compliance Requirements***

Both Deep Security and SecureCloud help to meet compliance requirements. Deep Security provides an integrated, cost-effective solution that addresses major compliance requirements for PCI DSS 2.0, as well as HIPAA, FISMA/NIST, NERC, SAS 70 and more. With SecureCloud, businesses can protect sensitive information in cloud, virtual environments, and physical infrastructure from theft, unauthorized exposure, or access when data is migrated to unapproved geographic data centers. This protection helps to support internal governance and ensure compliance with regulations like HIPAA, HITECH, Sarbanes-Oxley, GLB and PCI DSS. And both solutions provide detailed, auditable reports to support compliance efforts.

## **VI. CONCLUSION**

Many companies are still in the midst of deploying cloud computing, and cloud requirements will change and evolve for each company over time. Businesses need a solution that will secure their physical, virtual, and cloud servers, application, and data to protect them throughout their journey to the cloud. And with a solution that protects across private, public, and hybrid clouds businesses can select the right cloud deployment for their resource needs and business objectives—without being hindered by security risks.

Trend Micro provides total cloud protection with Deep Security and SecureCloud. Together, these solutions provide a holistic approach to cloud protection to mitigate the risks of data breach, theft, and data motility. Deploying protection 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.

## **VII. 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 Trend Micro Smart Protection Network cloud computing security infrastructure, our industry-leading cloud-computing security technology, products, and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe.

Additional information about Trend Micro Incorporated and the products and services is available at [TrendMicro.com](http://TrendMicro.com).

©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\_TotalCloudProtection\_110815US]

