VIRTUALIZATION AND CLOUD COMPUTING

SECURITY BEST PRACTICE

TREND MICRO™

Securing Your Journey to the Cloud

Introduction

To address the security threats and issues relevant to cloud computing and virtualization [1], this guide outlines recommended security best practices in virtual and cloud environments. For virtualized environments, private clouds, portions of hybrid clouds, and public Infrastructure as a Service (IaaS) deployments, the enterprise, not the service provider, needs to assume responsibility for security.

For example, enterprises need to control the deployment of Virtual Machine (VM)-specific security (see section below on self-defending VM security). In addition, the enterprise needs to control their encryption keys (see the section below on encryption). This ensures exclusive access to decryption controls and allows them to switch cloud vendors (i.e. avoid vendor lock-in).

When a service provider is used, part of assuming the responsibility for security includes determining what security the service provider offers for the underlying infrastructure. What certifications does the service provider have? Does the service provider follow any current cloud computing security standards? What level of visibility or transparency is provided into the underlying infrastructure configurations and security? While cloud vendors control certain security elements, the burden is on the enterprise to ensure that security provisions meet the business's security requirements.

Virtualization and cloud computing security best practices:

- Self-defending VM security
- Layered coordinated defenses
- Security optimized for virtual and cloud environments
- Visibility, reporting, and auditing
- Encryption for virtual and cloud environments
- Security that travels with data

Self-Defending VM Security

VM-level protection is crucial in a virtualized or cloud computing environment. By creating a security perimeter around each VM in this way, the enterprise can co-locate applications with different trust levels on the same host and can defend VMs in a shared, multi-tenant environment. This enables enterprises to maximize the benefits of virtualization, for example. And VM-level protection allows VMs to stay secure in today's dynamic data centers even as VMs travel between different environments – from on-premise virtual servers to private clouds to public clouds, and even between cloud vendors.

Layered Coordinated Defenses

A variety of distinct security technologies should be deployed to achieve comprehensive VM-level security that increases protection and maintains the compliance integrity of servers and applications, whether in virtual or cloud environments. These include security layers such as firewalls, intrusion detection and prevention, file integrity monitoring, log inspection, and anti-malware protection.

- A **firewall** decreases the attack surface of virtualized servers in cloud computing environments. A bi-directional stateful firewall, deployed on individual VMs, can provide centralized management of server firewall policy. It should include pre-defined templates for common enterprise server types.

- **Intrusion detection and prevention systems (IDS/IPS)** intervene against attacks that attempt to exploit known vulnerabilities long before patches are published or deployed. Implementing IDS/IPS within the virtualized environment can shield applications and operating systems from newly discovered vulnerabilities. This achieves timely protection against known and zero day attacks. In particular, vulnerability rules shield a known vulnerability – for example, those disclosed monthly by Microsoft – from an unlimited number of exploits.

- **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.

- **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.

- **Anti-malware protection** defends against viruses, spyware, Trojans and other malware. It should detect malware in real time and incorporate cleanup capabilities to help remove malicious code and repair any system damage caused by the malware.

Security Optimized for Virtualized and Cloud Environments

Security solutions should offer both agent-less and agent-based security options to provide flexible deployment alternatives and close security gaps unique to virtualized and cloud environments. Agent-less security is ideal for virtual infrastructures and private clouds. By leveraging hypervisor introspection application programming interfaces (APIs) such as the VMware VMsafe and vShield Endpoint APIs, businesses can now deploy a single antivirus engine to a dedicated security virtual appliance and deploy a very small footprint driver in each VM to perform the necessary offload. This provides the following advantages:

- Ensures other guest VMs are secure when dormant and receive the latest pattern file updates whenever activated.
- Enhances virtual server performance by running resource-intensive operations such as full system scans from the separate scanning VM and staggering guest VM scans.
- Offers agent-less anti-malware, file integrity monitoring, host-based intrusion prevention, Web application protection, application control, and firewall as agent-less security options.

In a virtual environment, agent-less security uses the dedicated security VM to eliminate the agents from the guest VMs and reduce the resource burden on the underlying host – preserving performance and increasing VM densities.

In a public cloud environment, businesses cannot use a dedicated scanning VM to protect other VMs because they do not control the hypervisor in a public cloud. Instead, an agent-based option provides protection on the VM level, creating self-defending VMs in a multi-tenant environment.

Security solutions should provide both agent-less and agent-based options to protect across both virtual and cloud environments, all managed through a single console. With this approach, businesses can optimize virtual and cloud resources, simplify administration, and reduce costs.

Visibility, Reporting, and Auditing

For security monitoring and reporting, and to support auditing, enterprises need granular visibility into security events and suspicious behavior. This is best achieved by implementing security that is integrated with virtual and cloud vendor APIs. Such integration may enable the security vendor to collect operating system and application logs at the VM level. This may also facilitate monitoring of inter-VM traffic across virtual switches. Armed with this visibility, enterprises can evaluate and remediate problems, develop procedures to avoid similar incidents going forward, and help meet regulatory compliance requirements.

Encryption for Virtual and Cloud Environments

Encryption addresses a range of security challenges related to virtualization and cloud computing. Standard 128-, 192-, or 256-bit encryption of storage volumes deters hackers from prying and thieving, and reduces the risk that the cloud storage devices could be sold or reused while they still contain confidential or private information. Encryption also greatly reduces the risk of malicious VM attacks; as long as the encryption key for the data stores have not been provided, even if rogue VMs reach data stores, volumes are unmountable and unreadable.

Encryption with enterprise-controlled key management enables IT to comply with security best practices, internal governance, and external regulation. Data is kept secure, and the key management solution can provide monitoring, reporting, and auditing capabilities that provide visibility into data access. As a result, enterprises realize a significant reduction in the scope of compliance audits.

Encryption for Virtual and Cloud Environments

In summary, best practices for encryption for virtual and cloud data protection include:

- Integration with leading cloud service providers and virtual environments.
- Policy-based key management that determines where and when encrypted data can be accessed.
- Identity-based and integrity-based server validation to determine which servers can access secure storage volumes and whether security is up-to-date on those servers prior to data access.
- Business control of encryption keys, either on-site or through a separate SaaS service, to maintain a strict separation of duties between the business and cloud service provider.

An encryption solution should provide native support for virtual and cloud environments, with key management provided through one console for all deployments. This allows businesses to encrypt their data with one solution even as their data center changes and evolves. And, enterprise-controlled encryption and policy-based key management enable portability between cloud vendors, as data security is not tied to any single cloud vendor.

Security that Travels with Data

In virtualized and cloud environments, more than ever before, security must travel with data, wherever it resides. One way to achieve this is via the VM-level security described above. The consumerization of computing increases the urgency for this sort of data protection. Roaming workers, traveling salesmen, and remote employees are increasing in number. They are using a widening array of devices to access data, including smartphones, tablet computers, netbooks, notebooks, and traditional laptops. VDI and cloud applications are accelerating this shift.

Cloud security must accommodate these shifting usage patterns by providing security at the diversity of endpoints. This includes both security for the cloud, protecting business cloud environments, and security from the cloud, providing cloud-based updates and threat intelligence for faster protection. Hence, a new paradigm of security is emerging that travels with the data wherever it resides and supports the elastic perimeter of the modern network. Security travels with the VM on premise in a virtualized environment, to the cloud, and extends data protection to our mobile endpoints.

More Information

For More Information

Learn more about securing your journey to the cloud.

- Trend Micro Cloud Security Blog: http://cloudsecurity.trendmicro.com/
- Journey Web Pages: www.cloudjourney.com
- White Paper: A Brave New Security World (by Trend Micro CEO, Eva Chen)

Follow these links for more information on specific security solutions for virtual and cloud environments:

- Security for Physical, Virtual, and Cloud Servers: Deep Security
- Data Protection Using Encryption with Policy-based Key Management: SecureCloud
- Virtual Desktop Security: VDI Solution Page

Reference

1. "Virtualization and Cloud Computing Threat Report." Trend Micro. August 2011.

TREND MICRO™ Securing Your Journey to the Cloud

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 www.trendmicro.com