The Challenge

Virtualization has added a new complication to the world of software licensing because the term “machine” in the conventional sense is no longer clearly defined. Virtualization allows a computer environment to be simulated in software, including most of the hardware resources which support that environment.

Licensing technologies struggle with this concept since they normally do not make a distinction between ‘real’ hardware and virtualized hardware. Most licensing technologies use the concept of hardware fingerprinting to prevent licenses from being copied illegally. If a virtual machine image is copied or cloned, the virtual hardware fingerprint (along with the copy-protected license) is also cloned.

The Sentinel RMS Solution

Sentinel RMS now includes two areas of distinct functionality designed specially with virtualization in mind.

VM Detection

VM detection allows an ISV to set a policy where an application’s license will simply be invalid if used within a virtual environment, or set a special condition such as charge customers a premium for running on virtual machines.

Additionally, the ISV can choose to prevent the license server from being installed onto a virtual machine, yet allow the workstations which are running the protection applications to be freely deployed within any combination of native and virtual environments.

End-User Benefits

Reduced capital and operational costs through more efficient use of hardware resources.

Reduction in power consumption, saving more money while reducing carbon footprint.

More efficient testing/development and security of systems.

Improved scalability and deployment agility for creating increased availability or bandwidth.

High availability/redundancy in managing a clustered infrastructure.

A pure software-based, electronic solution - authorize and control software in any virtualized environment with the industry's first and only technology-agnostic VM binding solution.
**VM Fingerprinting Options**

RMS now includes two new locking attributes designed specifically to address the problems of license duplication within virtual environments.

**CPU Info**

- This is a collection of CPU related attributes which are combined into a single fingerprint to represent a computer’s CPU as uniquely as possible.

- The CPU of the virtual machines’ host computer is one of the few components that is not virtualized, and therefore any CPU characteristics obtained from within a VM will be taken from the ‘real’ CPU.

- This allows RMS to create a binding between the virtual machine and the physical hardware.

The “CPU Info” is based on multiple CPU related properties (CPU name, manufacturer/vendor, model, family, stepping) and the probability of multiple machines having identical CPU signatures is low. Alone, it does not provide a sufficiently unique fingerprint, but, when combined with a locking attribute such as MAC address, it provides a sufficient level of protection within normal business environments.

**UUID (Universally Unique Identifier)**

- This is a standardized software identification component and is used as a means of unique identification with the majority of VM technologies. It consists of a 32-character hexadecimal number.

- It can be used to identify a specific virtual machine image, and can be retrieved from the VM while it is running.

UUID should be considered a ‘soft’ locking option and is better suited for upholding compliance enforcement rather than protecting from serious malicious intent.

**Licensing in centrally managed virtual infrastructures**

Centrally managed VM infrastructures (also known as server based infrastructures) add the concept of hardware clustering to virtualization. Here, the VM infrastructure does not always leverage a single, fixed set of physical hardware resources, and will instead utilize a shared pool of resources.

For centrally managed cases, binding a license to the CPU info is usually considered to be a robust mechanism. For the most common type of clustered deployments where live migration capabilities are needed, there is usually a requirement for all the physical machines within the cluster to have the exact same CPU configuration. Solutions such as VMware’s ESX also include the ability to enable CPU masking to improve compatibility in high availability and fault tolerant setups. This will allow different physical CPU configurations to be used, yet present a common (masked) CPU configuration across all of the physical machines. Therefore, the fingerprint based on CPU info will not change when the VMs migrate across the cluster.
However, some centrally managed deployments will allow the CPU characteristics to be different (for example, with cold migration cases where VMs are shut down before they are migrated). In these cases, locking to the CPU info will not work since there is a high chance that the CPU details will change. To solve this, the license fingerprinting needs to be based on attributes that remain fixed despite changes being made to the underlying physical hardware.

This is an area where locking to UUID has a lot of value, since in normal circumstances, it can be treated as an attribute which is unique and fixed to a specific virtual machine.

As long as an administrator uses the VM vendor’s supplied tools to manage the cluster, each virtual machine will have its own unique UUID assigned to it in a persistent way. If a virtual machine is cloned within the cluster, a new UUID is automatically assigned to it, and if a VM is moved out of the cluster, the UUID will move with it.

However, if a vendor attempts to manage the cluster manually, the UUID values can be edited and changed, which is why this is a solution for compliance enforcement, not protecting against piracy.

Choosing your locking strategy

In most cases, an ISV does not want to make a decision regarding the type of VM deployment a license will be installed onto at the time of order fulfillment. ISVs who seek a generic strategy that will apply to any possible installation should use the following:

- “CPU info + MAC” address as the primary fingerprint. UUID could also be included as a third option in this fingerprint.
- “UUID + MAC” address as a secondary (backup) fingerprint

The above combination will ensure that any deployment is adequately handled, yet a high level of protection against license duplication is maintained. If the primary fingerprint is invalidated due to a hardware change, the secondary fingerprint is used to validate the license. Although the UUID does not provide strong piracy protection, it still provides the highest level of compatibility for almost any VM deployment setup, from standalone/workstation VMs to large-scale fault tolerant clustered setups.

Technical Specifications

At the time of writing, the VM detection and VM fingerprinting capabilities provided by Sentinel RMS have been validated on the following technologies:

- VMWare Workstation v7.0
- VMWare ESXi v4.0
- Virtual Box v3.1
- Virtual PC 2007 v6.0
- QEMU v0.11
- Parallels Desktop 4
- XEN Hypervisor 3.2
- Microsoft Hyper-V Server 2008 R2
- KVM 76

It should be noted however that the fingerprinting strategy of combining CPU info with the MAC address works independently to the underlying virtualization technology and can therefore be considered to be agnostic to all current technologies.