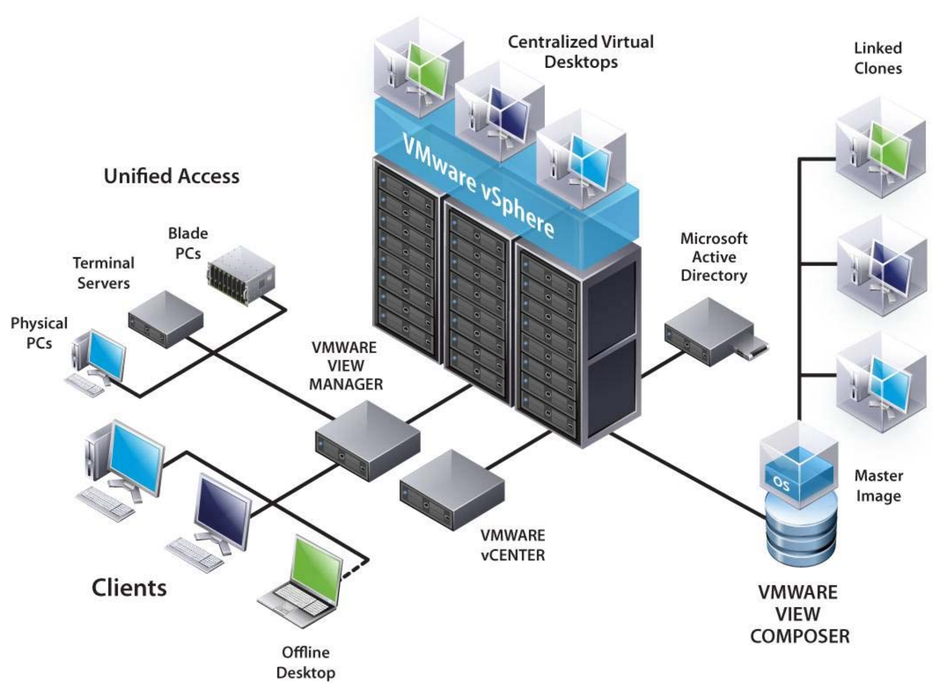
Cloud Forensics: An Investigation into Imperfect Virtualization (Work in Progress)

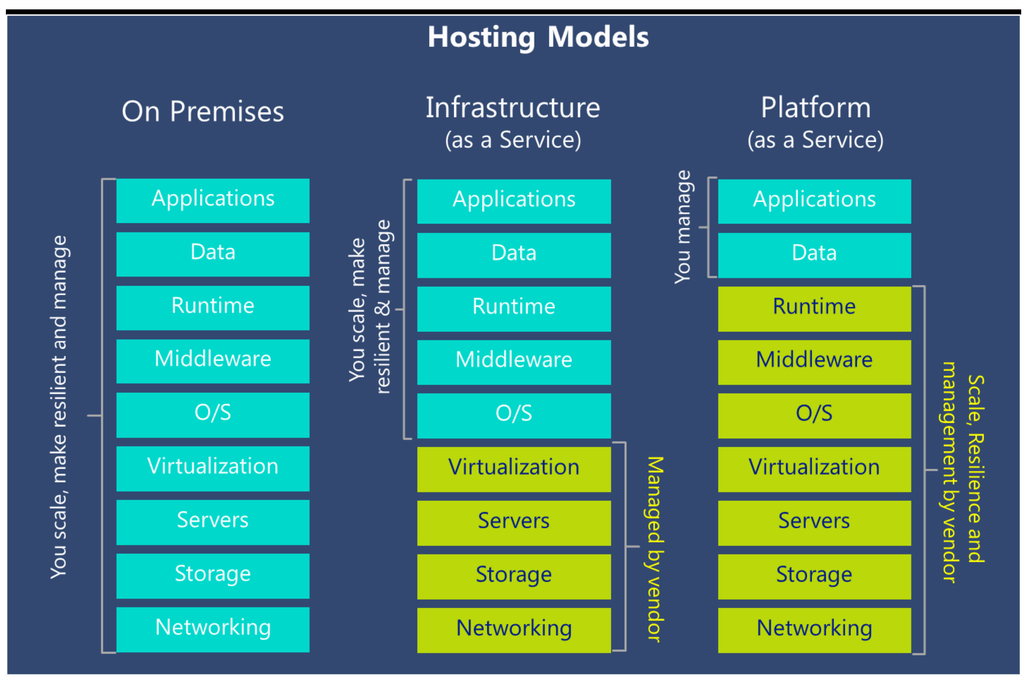
Eric Katz, Dr. Samuel Liles

Problem Statement

Cloud computing is becoming more popular and companies are quickly adapting cloud strategies as a cost saving means. Unfortunately, this also means that they are putting information onto cloud servers and devices without realizing the security implications. An essential characteristic of cloud computing is resource pooling. This sharing requires that each instance be segregated. Virtualization is the key technology that allows this to occur.

If this virtualization and segregation is not done properly there could be huge ramifications. Depending on how the instantiations are made, data from previous virtual machines could be located in unallocated sectors or within the RAM of a different running instance.

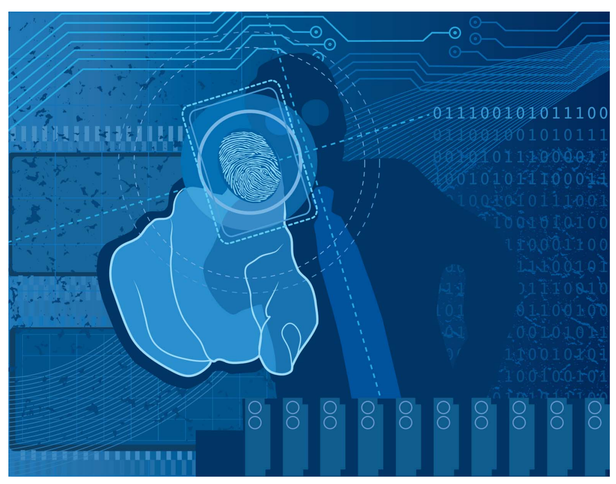




Experiment and Methodology

Create a Windows 7 VM using IaaS from Microsoft Azure.
Use multiple forensic imaging techniques to copies of the VM and the RAM
Examine the images for data that does not belong to them in the unallocated space and RAM

Hardware
iMac running Windows 7
Azure – (Unknown)



Software
EnCase
FTK
FTK Imager/Lite
Memoryze
Redline
HxD
Winhex Forensic Edition

Expected Results

Using hex editors and data carvers to examine the unallocated space from the VMs will reveal non 0 data.
RAM will contain data difficult trace the origin to something other than the instance.

If data is found that does not belong to the instance then there is a huge security concern. This will have been a previously unidentified attack vector that puts potentially sensitive customer data at risk and could make service providers liable.