

Much discussion has gone into the topic of securing the virtual infrastructure based on issues such as 1) the virtual switch is now invisible, 2) entire servers have become files, 3) the hypervisor is a new threat surface, 4) the virtual administrator has been given the keys to the kingdom, all with no oversight and/or a new concept around virtual physical access. What do these really mean, and how can we protect against them?

We first need to define and understand virtualization and what has changed. Virtualization is one of those computer terms that is often overused and misunderstood. Wikipedia defines it as follows: “*Virtualization* is the creation of a virtual (rather than actual) version of something, such as an operating system or computer.” You can have network virtualization, storage virtualization, desktop virtualization, operating system level virtualization, full virtualization, and more. All of these have nuances. With that in mind, we will focus on virtualization of the datacenter and desktop environments, or full virtualization.

Consolidation, flexibility, disaster recovery and business continuity with significant cost savings are all drivers of the virtualization. All of these considerations are very important drivers on their own, but together they create the perfect storm for IT directors to pull out all the stops and implement, possibly without complete consideration. We have seen 145% ROI with payback in less than two years, with cost savings in power, space, cooling, and HA/DR, delivering faster cheaper solutions.

To get in the way of these savings is futile. (It’s no wonder that security has been a bad word in this process for a number of years). **There is no free lunch!** With all of these benefits comes some serious concerns and issues from a security perspective. However, it is not all bad news. With the right controls, the virtual infrastructure actually becomes more secure.

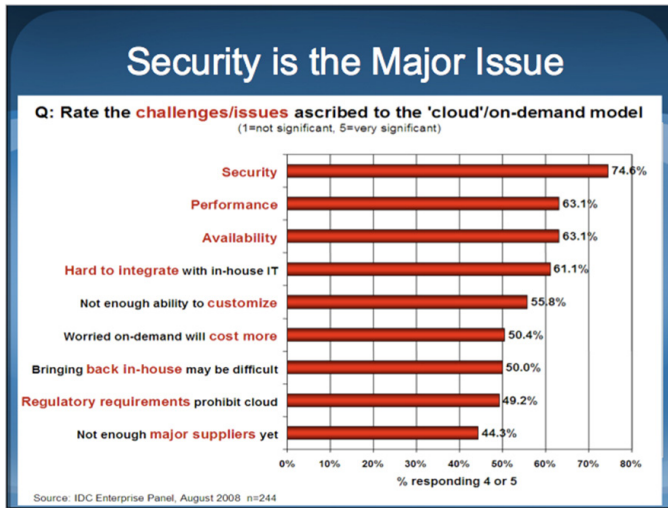
Virtualization has created a number of new gaps and concerns, including consolidation, server becoming files, hardware is now software, and VMs are mobile, with the new concept of virtual physical access.

Consolidation into the memory backplane of big servers has created a visibility issue. Security professionals will tell you that you can’t protect what you can’t see. Consolidation of roles and functions in the datacenter has created a separation of duty issue with the administrative function, which creates a serious violation of best practices and regulatory controls in the datacenter.

Servers become files creates incredible flexibility from duplicating virtual machines within seconds. Backup and recovery is a matter of duplicating files, but again, with these benefits comes concerns, such as, where is my data? Someone could copy the entire machine onto a USB drive and walk out of the datacenter with your virtual machine, run that machine on their own virtual infrastructure, and attempt a brute force attack and escalation of privilege. Life cycle management can be a very real issue with duplication of virtual machines, meaning the non-repudiation can become impossible because someone accidentally made two copies of a production machine. VM sprawl is almost inevitable, which will ultimately affect the scalability and performance of the environment.



Securing the Virtual Infrastructure and the Cloud



Hardware is now software has many benefits and features never dreamed about before, like v-switch, new state, snap-shots, instant roll-back, differential instances, vmotion and dynamic spillover into the cloud, which is covered in more detail under **Virtual machines are mobile**. We see how the v-switch has created great flexibility and productivity when managing the network in the datacenter, but how it potentially flattens the network and breaks the segmentation of the network, negating zones of trust or communities of interest. New states, like suspending a virtual machine, means that you need to rethink the process of scanning for vulnerabilities, AV and malware because most scanners require the machine to be running when the scanner looks for issues. We have also seen a major issue develop in the virtual infrastructure around AV storm, which is being addressed by most of the major AV vendors, but will develop as vendors look to solve the problem. Now, what about snap-shots, instant rollback, and differential instances, which again, have incredible benefits to the flexibility, speed to deploy, test and QA? Again, **no free lunch**. What about managing this environment and dynamic nature? For example, what is being done from a lifecycle and non-repudiation perspective? Who is using that instance and why do they have access? These are all becoming relevant - consideration on the roll-back feature that allows attackers the ability to cover their tracks by rolling back, or issues like the crypto technology, which is potentially vulnerable.

Virtual machines are mobile. This concept is the most amazing feature that enables a whole new paradigm of cloud computing and hybrid solutions. Virtualization is the key technology to enable the cloud. What is the cloud? NIST defines it as: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential **characteristics**, three **service models**, and four **deployment models**. We will go into detail in the cloud section of this whitepaper to look at the characteristics, service models and deployment model and how they impact security.

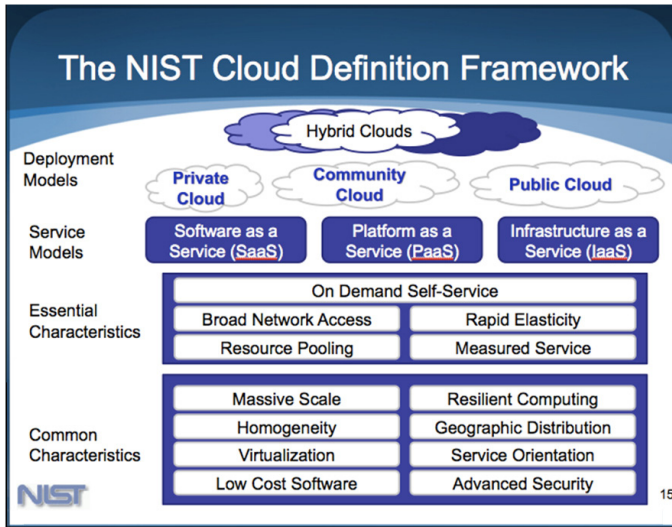
Cloud or Virtualization security is all about visibility and control which start with tools to effectively manage and see the scaling, software lifecycle, diversity, mobility, identity and transient nature of the virtual infrastructure.

The cloud is all about enabling organizations to scale by handling things like velocity and to be incredibly flexible without need to make huge capital investments. Again, we believe it comes back to saving money, or to the fact that making money defines a solution's success. Therefore, if organizations have incredible benefits and it helps them make more money or save money, companies will buy. One caveat is that they do not have any major risks when implementing the solution, and the cloud scares folks from a security and control perspective. We are seeing the initial user of the cloud using it as a development platform option, and some start-ups are using it because it limits the capital requirements.

The cloud and managing the use of it comes with some very real issues. We were working with an advertising agency who had their Rackspace VM server hacked and then used it to launch attacks against the Amazon cloud. What was interesting was that the hack was able to escalate privilege, but because it was a development server, and no sensitive data was on their machine, the hacker decided to use it as a vehicle to attack other machines.

The cloud is going to re-introduce simple overlooked security issues like default user and password, unnecessary open ports, default configurations and other issues we

Securing the Virtual Infrastructure and the Cloud



thought we had solved. When someone else sets up a VM for you, you can never truly be sure that it is secure, so we need to have hardening best practices outlined.

The cloud is truly going to change business as we know it. If we can get past the regulatory and security issues, we believe we can do that with the right defense-in-depth strategy and tools.

Solution

The defense-depth-solution requires taking a step back and realizing that no matter what we do, the bad guys are always going to be smarter than us, and will find a way to escalate privilege, given enough time and access. Ensuring that we are monitoring and alert with good actionable information is the first step. Locking down the environment with white and black listing is also key. Hardening the VM with minimal open port and service and a host based firewall, HIPS, and ensuring the VM is encrypted at power-off state are also absolutely necessary.

The tool that brings this all together is a SIEM (Security Information and Event Management) tool. Correlation of information from logs and alerts is crucial in effectively securing the virtual infrastructure.

The other key tool is an application white listing and file integrity product which will ensure files and applications are not changed and/or the integrity is maintained at all times.

We will see organizations use many virtsec solutions which

will work in different environments, whether the investment is VMware, Xen or HyperV. But the best generic approach is to leverage a SIEM and File/application integrity solution. This will satisfy the most comprehensive audit, incident response, authentication and access control of regulatory requirements from all the frameworks, whether it is FISMA, PCI and or SOX.

Securing the Virtual Infrastructure (VI) is about visibility of the events and activities on the hypervisor and manipulation of the virtual infrastructure, whether it is v-switch or virtual machine. As we mentioned before, you have a new concept to deal with called “virtual physical access.” We all know that if someone obtains physical access to a machine, they will own it. That is why we have physical security at the datacenters. Virtualization allows you to obtain access to a virtual machine and manipulate it as if you had physical access because storage, networking, and even memory are just an api call. So if you escalate privilege in the Virtual Infrastructure, you own the virtual datacenter. Therefore, base-lining and watching for specific activity in this dynamic environment is critical in order to be alerted of the malicious insider or an attack.

Software is always going to be vulnerable and the bad guys will find the vulnerabilities and exploit them, but whether it is an insider or attacker, once they have escalated privileges, they have to do something in the environment to affect access to data. And if you have followed best practices to harden the environment, when they make changes, those changes will be detected. Security Events, Logs and Alerts that are effectively correlated will provide actionable information for the security team to manage. The VI is so dynamic and flexible that it would be completely impossible to manage without an automated correlation engine.

SIEM tools, which continuously gather log information from network devices (through syslog protocol, SNMP traps, and other adapters), offer a highly cost effective way of furnishing visibility to network usage and operations. SIEM tools track user logins, policy changes, and other user activity. This provides a large amount of visibility and security awareness using standard techniques that are relatively simple to implement. In recent years, this class of tools has become the predominant “portal” for security awareness, and an essential part of security operations for



all enterprises. Many security specifications, including PCI-DSS, mandate the implementation of SIEM tools within an enterprise.

SIEM will address 80% of Security and Compliance issues and gaps, providing visibility and control to all the major concerns.

CorreLog has developed a number of templates and alerting framework to help navigate the different issues. CorreLog can work with your current investment in Catbird, Hytrust, Reflex, Altor or VMware vshield zones to ensure 100% coverage.

CorreLog not only monitors all of the underlying operating system events, it also monitors the hypervisor itself for security events and breaches.

CorreLog, a McAfee SIA partner, also provides a complete integration with EPO from McAfee which address the endpoint security offering, allowing for correlation of events from McAfee to be correlated with all other events from the enterprise. If you want to secure the machine in the public cloud you will have to harden the virtual machine with encryption, firewall, HIPS, etc., and then report to the CorreLog SIEM. The public cloud has limited access to the underlying hypervisor information, so again, CorreLog recommends you watch the account log information and correlate that with VM security events and information from end-point software.

About CorreLog, Inc.

CorreLog, Inc. delivers security information and event management (SIEM) combined with deep correlation functions. CorreLog is real-time, SIEM software that automatically identifies and responds to network attacks, suspicious behavior and policy violations. CorreLog collects, indexes and correlates user activity and event data to pinpoint security threats, allowing organizations to respond quickly to compliance violations, policy breaches, cyber attacks and insider threats. CorreLog provides auditing and forensic capabilities for organizations concerned with meeting SIEM requirements set forth by PCI/DSS, HIPAA, SOX, FISMA, GLBA, NCUA, and others. Maximize the efficiency of existing compliance tools through CorreLog's investigative prowess and detailed, automated compliance reporting. CorreLog markets its solutions directly and through partners. Visit www.correlog.com for more information.

CorreLog, Inc.

311 Conners Avenue
Naples, Florida 34108
Phone: 1-877-CORRELOG
239.514.3331
Email: info@correlog.com