



**WHITE PAPER: Cloud Computing**

# Securing Virtual Compute Infrastructure in the Cloud

Ken Owens

Vice President, Security and Virtualization Platform Technology, Savvis

## **Table of Contents**

2	Introduction
2	New Threat Vectors Introduced by Server Virtualization
4	Architectural Considerations
8	Virtual Security Architecture
12	About Savvis

### Introduction

Server virtualization is one of the hottest topics in IT today. Initially driven by the need to consolidate servers to achieve higher hardware utilization rates, boost operational efficiency, and cut costs, enterprises more recently have implemented virtualization to get on-demand access to additional compute resources. This enables them to add processing and storage capacity on the fly as needed to respond to changing business conditions. Because virtualization allows them to move resources from congested to less-congested hosts as required, enterprises also get improved server reliability, which in turn increases application performance. And consolidating servers through virtualization helps companies achieve the “greener” data center operations increasingly mandated by corporate sustainability programs.

Despite these benefits, there are challenges — specifically, security challenges. Conventional infrastructure security controls designed for dedicated hardware do not map well to virtualized environments. To address these challenges, virtual infrastructure architectures must have well-defined security policies and procedures in place. Additionally, although they probably will never be fully interoperable with existing dedicated security controls, there has to be some degree of compatibility between the newer security protections specifically designed for virtualized environments and traditional controls.

This white paper first discusses the most common unaddressed security issues in virtualized infrastructures. It then explains how Savvis' Cloud Compute family of products delivers security services that address these issues. Finally, it presents a cloud security services architecture virtualization strategy that enterprises can deploy to get the most out of Savvis' Cloud Compute offerings.

### New Threats Introduced by Server Virtualization

Most of the new security threats introduced by server virtualization environments arise because of the difficulty of securing virtual machines (VMs) both prior to deployment and during day-to-day operations. And, as when implementing any technology, process and people issues also contribute to the challenges of effectively mitigating those threats.

### Technology Concerns

Before deploying virtualization, enterprises need to recognize that the host operating system in a virtualized environment is a new, privileged layer of software. This layer will be the target of security attacks. Although this software layer is “thin,” it is still an operating system, and therefore despite the fact that enterprises should experience fewer security issues overall, their systems will still be vulnerable.

The two main threats that target this layer are VM escapes and VM hopping. VM escapes are security attacks designed to exploit a hypervisor. Once successful, a VM escape attacks other virtual machines that reside on the same physical host. Alternatively, a VM hopping attack is when one VM is able to gain access to another VM using vulnerabilities in either the virtual infrastructure or a hypervisor.

## WHITE PAPER: Cloud Computing

Another security vulnerability occurs when enterprises attempt to patch offline VM images. Current patch management tools cannot do this, making updating signatures and protecting offline VM and VM appliance images from tampering difficult. Additionally, it is important to understand the lifecycle of the VMs and their changes in states as they move through the environment. VMs can be on, off, or suspended. VMs can also be unallocated in storage, with no state associated with them. It is important to continually assess a VM's vulnerabilities and apply updated security patches to VMs that are off, suspended, or unallocated.

Another threat arises from having no virtual network discovery capabilities or methods to baseline the configuration of a virtual server. Ideally, the virtual network, all VMs, the virtualized network devices, and all services — as well as their relationships and communications flows — would be discoverable. The support system should then automatically collect the discovered information to confirm correct configuration and form the baseline for future monitoring. This is not yet possible, and thus the vulnerabilities associated with configuration management of offline VM images raises serious security issues.

Additionally, virtualized environments provide limited visibility to inter-VM traffic flows. These traffic flows are not visible to traditional network-based security protection devices, such as the network-based intrusion prevention systems (IPSs) located in the data center network. A virtual IPS solution, integrated with the hypervisor, would prevent communication directly between hosted partitions within the virtual server. To secure the virtual infrastructure, virtualized security capabilities are required to be inline to the virtual network and between the guest operating systems to provide visibility and protection against attack. The challenge is that signature, filters, and rule updates are needed for offline VMs. In addition, VMs must be protected from tampering while VMs are in motion.

One of the primary advantages of VMs is that enterprises can move them around the physical environment as needed to get more processor or compute resources. But mobile VMs need security policies and baseline histories to move with them. When a VM moves, if the security policy does not accompany it, that VM becomes vulnerable. In addition, when VMs move, they lose their performance histories and their baselines need to be re-evaluated. This raises a serious question: How should security policy history be maintained on individual mobile?

### Process Concerns

In a physical environment, organizations separate the administration of server configurations from the administration of network, security, and storage configurations. This process is called segregation of duties (SOD). However, in a virtual environment, SOD is no longer considered necessary because the VM environment exists within the server environment.

This raises concerns because the organization now has two separate policies: one for the physical environment and one for the virtual environment. Policies defined by security administrators are not being governed by them in the virtual environment. Although server administrators are very good at administering server policies, they frequently do not have the appropriate level of security training or experience.

## WHITE PAPER: Cloud Computing

Moreover, the auditing community is increasingly convinced that current practices for auditing VM movements, changes, and lifecycles are inadequate. As compliance grows in importance, enterprises implementing virtualized environments need to satisfy their auditors' concerns, especially since creating an identity for an individual VM and tracking that VM from creation to deletion creates challenges for even the most mature virtualized environments. This is greatly complicated by VM sprawl, or the situation where the number of VMs being created is growing more quickly than an enterprise's ability to manage them.

### People Concerns

As with any new technology, implementing virtualization raises people as well as technical and process issues. With virtualization, the primary personnel-related challenge has to do with knowledge of and experience with the environment. For example, current virtualization security and management tools are very rudimentary, very immature, and security staffs are often not familiar with them. Indeed, most of the tools that security staffs are familiar with do not work in the VM environment at all.

As a result, organizations implementing virtualization need to educate their security provisioning and support staff on VM environments. They must also help server, network, and storage administrators understand the technology and process challenges of virtualized environments.

### Architectural Considerations

The challenges outlined above cannot be met by deploying existing technologies or processes. Neither is there a single solution that will address all of them. Rather, enterprises need to deploy a holistic architectural security strategy that encompasses all three aspects of a successful virtualization implementation.

Savvis understands that. We take a different approach to security by integrating it into all our products instead of bolting it on at the end or as an after-thought. This enables Savvis to deliver flexible security services at a reasonable price. Specifically, our Savvis Cloud Compute platform delivers these flexible services via a secure VM infrastructure.

### Security Agility

One of the common misconceptions about security controls is that they can lock down an environment so tightly that the business functionality of a system or application is crippled. This does not have to be the case. By architecting security controls into an infrastructure up front, the business functionality can remain intact without compromising security.

With virtualization, the mobility of VMs is one of the most important attributes. But enabling VM mobility in a physical infrastructure that is not aware of the virtualization layer is very difficult. Enterprises must take into account that in a virtualized environment, the security controls, systems management infrastructure, and server management infrastructure have all been integrated.

## WHITE PAPER: Cloud Computing

Enterprises shouldn't relax their compliance and security efforts in virtualized environments even though controls that exist in the physical server environment are missing from the virtualized one. That's why a key feature of the secure VM architecture developed by Savvis — which is the basis for its Cloud Compute platform — is that both the physical and virtual compute environments are equally agile. Enterprises can move VMs around the Savvis hosted compute infrastructure in a secure manner while maintaining the same policy controls as in a physical environment.

Savvis' Secure VM architecture gives enterprises the same degree of visibility and control as they get with a dedicated architecture through the SavvisStation customer portal. This portal is also much more feature-rich than traditional virtualization management components like VMware's infrastructure client. Figure 1 demonstrates the visibility provided by Savvis' secure VM architecture — including visibility into VMs that are powered off or which are sitting unassigned in a storage pool.

The screenshot displays the SavvisStation interface for a virtual machine named 'samplewin'. The interface includes a navigation menu on the left with categories like 'Data Center', 'Application Servers', 'Web Servers', and 'Security Policies'. The main content area is titled 'Virtual Machine Information' and contains several sections:

- General Information:** Lists details such as Guest OS (Microsoft Windows Server 2003, Enterprise Edition (32-bit)), Memory (300MB), State (Powered On), CPU (2), IP Address (10.12.156.60), Host (10.12.156.13), Current Network (VM Network), Device Config (ID: 4000), IP Address (10.12.156.60), Mac Address (00:50:56:0b:32:d3), romulus:storage1: Used Capacity: 393GB, Free Capacity: 257GB, and Customer (Customer).
- Performance Statistics:** Shows progress bars for CPU Average Use (MHz), Network Average Use, Disk Average Use, Memory Average Use, and Active Memory Average Use.
- Control Central:** Provides buttons for Power OFF, Connect, Reboot, Suspend, and Reset.
- Policies In Effect:** Lists active policies such as 'Prohibit access to properties of LAN', 'Ability to delete all user remote access connection', and 'Turn off automatic update of ADM files', each with an associated 'Audit Report' link.
- Storage Options:** Includes links for 'ILM Storage View' and 'Storage Performance'.

The footer of the interface shows the copyright notice '© 2008 SAVVIS, Inc. - All rights reserved' and the login information 'Login: SAVVISStation Demo (Administrator)'.

Figure 1

# WHITE PAPER: Cloud Computing

Figure 2 shows the level of policy control the Secure VM architecture provides. The policies can be selected from the defined global policies, or can be modified to better match other desired requirements.

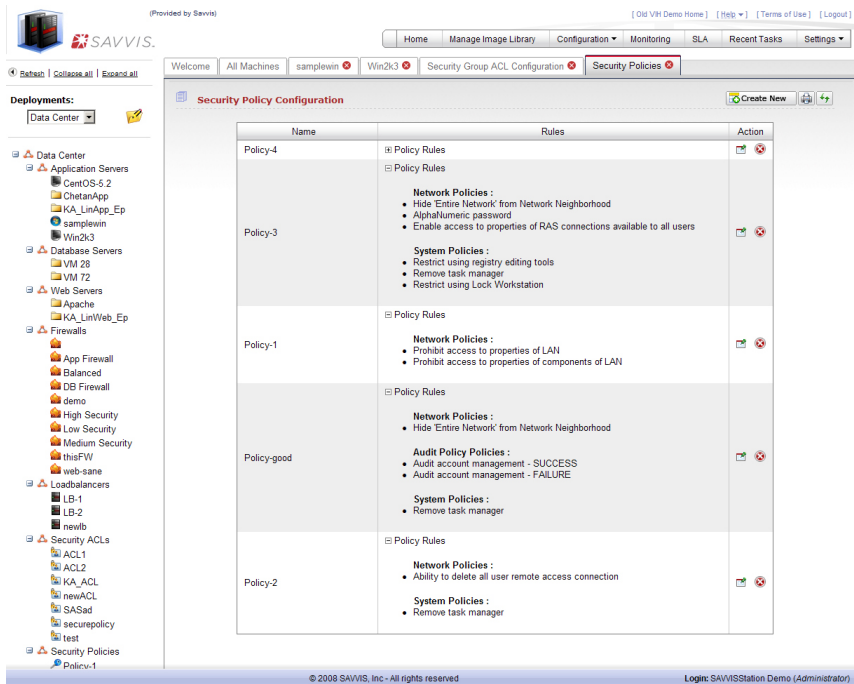


Figure 2

The Secure VM architecture was developed from the beginning to provide audit controls around the mobility of VMs. A sample audit report is shown in Figure 3.

Policy Name	Last Occurrence	Priority	Description
Prohibit access to properties of LAN.	2009/02/20 09:10:11 AM	2	Access to the LAN properties prohibited.
Ability to delete all user remote access connection.	2009/02/21 09:10:11 AM	2	Remote access connection could not be deleted.
Turn off automatic update of ADM files.	2009/02/22 09:10:11 AM	2	Automatic update of ADM files is blocked.

Figure 3

### Defense in Depth

Strategies for ensuring perimeter security have evolved significantly over the last few years. Today, most enterprises have deployed layered defense strategies, but server virtualization has complicated matters. Most organizations, in an attempt to consolidate servers, have left themselves vulnerable to the inter-VM communications that exist because if one VM is compromised, then all the other VMs that are part of the virtual network can be compromised without anyone detecting it. To ensure that each layer of the infrastructure possesses equivalent security controls, Savvis' Secure VM architecture provides layered security components in both physical and virtual environments.

By providing virtual security services from within the virtual server infrastructure, Savvis enables enterprises to deploy security policies and rules between each VM (or between VM farms) as they would in the physical world. And a key feature of the Savvis Secure VM architecture is that enterprises can move these security policies and the data collected about them with the VMs. This allows them to consistently enforce security services.

In addition, by design the Secure VM architecture provides security services on the hypervisor's virtual infrastructure layer. This enables virtual switch connectivity to the physical infrastructure and management network, and ensures that the hypervisor doesn't get compromised.

### Patch Management

One of the biggest compliance challenges related to managing security within both physical and virtual infrastructures is patch management. Although a number of software solutions and processes can help enterprises manage patches in the physical world, there are major gaps in the solutions available for the virtual one. A number of key questions have not been answered, including:

- What is the current patch level of the VM state – offline, off, or suspended – and the known vulnerabilities and patches for the VM?
- What is the risk of having unpatched VMs?
- If this VM image in the storage pool is turned up, what vulnerabilities in the environment does it expose?

Enterprises have tried various ways to deal with patch management in a virtualized environment. For example, some enterprises power on and patch on a predefined schedule, or require a VM to power on only in a demilitarized zone (DMZ) that can remediate before releasing the VM to production. Another solution is to not allow offline VMs in the infrastructure. But these solutions limit the availability of virtual servers and can hinder organizational agility.

Savvis' Secure VM architecture offers a policy control service that can provide some offline patching. It integrates with an enterprise's existing server management platform to ensure consistent policies are adhered to in both the physical and virtual environments. This service can investigate the pool of VMs – whether suspended, off, or sitting on the storage area network (SAN) – and perform a risk analysis of the pool. Any identified risks can then be mitigated in an appropriate manner.

### Vulnerability and Configuration Management

Virtualized security architectures must include sufficient vulnerability and configuration management capabilities. The Savvis Secure VM architecture allows enterprises to identify not only the type of VMs that are running or available, but also how they are configured with regard to users, applications, and services. And all this can also be accomplished without the VM running, as the architecture provides a mechanism to perform what-if analyses to check the configuration state and potential vulnerabilities from starting the VM on a target system.

Additionally, the Savvis Secure VM architecture is completely integrated with the Savvis Threat Management Architecture to provide end-to-end vulnerability and threat management correlation and resultant policy configurations.

### Identity and Access Management

Payment card industry (PCI) auditors are very concerned about VM environments' lack of control over user access. Savvis' Secure VM architecture defines a VM identity that ties each VM to an identity within the Savvis managed infrastructure. Based upon this identity, Savvis is able to assign user, role, and privilege access within the virtual infrastructure to provide role-based access controls.

Enterprises also want to prevent unauthorized cloning or copying of the data on a VM to a USB device or CD. Savvis' Secure VM architecture can prevent the VM from being cloned or copied by utilizing a combination of the VM identity and server configuration management policies.

### A Virtual Security Architecture

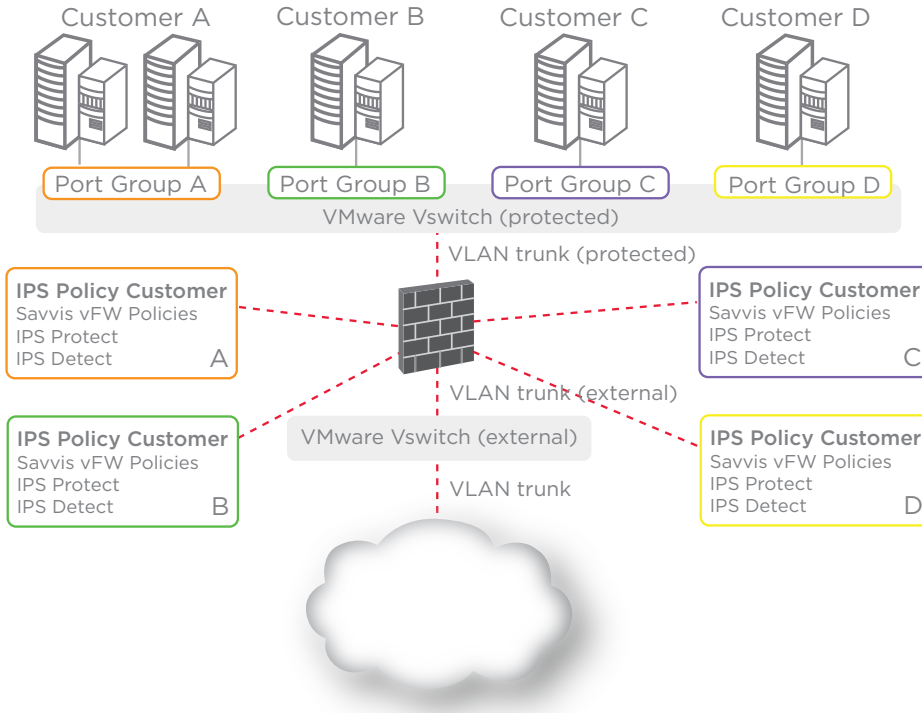
A virtual security architecture must defend enterprises against the new threats introduced by virtualization while maintaining performance and organizational agility. Savvis' Secure VM architecture is made up of two distinct sub-architectures:

- Secure VM Policy Services Architecture
- Secure VM Threat Management Services Architecture

The Secure VM architecture in turn is a subset of the Savvis Security Architecture<sup>1</sup> (SSA). SSA consists of policy management, utility network, utility compute, and utility storage architectural service components. Each of these architectural components, and their virtualization elements, is defined in greater detail below.

The Secure VM architecture is displayed in Figure 4.

**WHITE PAPER: Cloud Computing**



**Figure 4**

Policy Services Architecture	Threat Management Services Architecture
Customer-defined policy management	Secure virtual infrastructure from VM escape and VM hopping attacks
Audit controls reporting	Provide inter-VM visibility and blocking through VIPs
VM identity and access policies	Deep packet inspection through vFW
Monitor guest OS configuration policies	Network access control
Enforce mobility policies	
Actively seek rogue/misbehaving VMs	

**Policy Management**

Policy management services are application run-time controls that assist with the discovery of advertised security services. They allow granular definition, monitoring, and application of security policies to govern the use of the underlying services.

## WHITE PAPER: Cloud Computing

The policy management service elements consist of:

- Identity and access management
- Federated identity
- Single sign-on
- Security configuration management
- Information security management
- Controls management
- Vulnerability management
- Incident management policy definition, enforcement, and reporting

The impact of virtualization on the policy management services component is addressed by the technology and process element architectures defined below.

### Technology Architecture

The identity and access management element provides a unique identity for each VM in the infrastructure. The lifecycle of this VM can then be monitored and reported on regardless of state. This allows Savvis to manage access control policies on the VM — where it can start up, what users are allowed access, and even in which systems it can run.

The security agility element can provide much-needed controls and policies to ensure the security of mobile VMs. In addition to monitoring the VMS, the security agility service delivers VM audit reports. By defining policies around VM identity and access with security controls and audit reporting, enterprises can mitigate the risk of VM sprawl.

### Process Architecture

The policy management component enables policy definitions that manage the movement of VMs based on resources, security policies, service-level agreements (SLAs), and roles. Some of the processes supported by this component include the ability to view — but not stop or suspend — VMs, and the ability to view and start VMs, but not stop them.

### Utility Network

The utility network component adds additional layered security between the cloud and the utility compute components. The utility network elements of the SSA consist of utility firewalls, forthcoming Intrusion Prevention System (IPS) Service functionality, and virtual private network (VPN) functionality.

The impact of virtualization on the utility network component is addressed by the technology and process element architectures defined below.

### Technology Architecture

The utility virtual firewall element provides the perimeter firewall for the data center. This element is the first layer of defense for a virtualized infrastructure.

## WHITE PAPER: Cloud Computing

### Process Architecture

A physical infrastructure has clear segregation of roles between network operations and hosting operations. In a virtual infrastructure, Savvis maintains this segregation in two ways: first, the Savvis network operations team defines virtual switch virtual local area network (VLAN) and IP addresses. Then, the Secure VM policies are defined by security operations.

### Utility Compute

The utility compute component is architected to provide security hardening of layered security attributes available for grid, high-performance, and virtualized computing infrastructures. The utility compute elements of the SSA will consist of application and Web-based (XML/SOA) firewalls, VM IPS, and Host-based Intrusion Prevention System (HIPS) Service functionality.

### Technology Architecture

The VM IPS element consists of the inline virtualized intrusion prevention services. The patch management element provides patch management of offline images and the ability to manage the policies around the patch levels that must be supported in order to bring up an offline image. Additionally, the file integrity of any guest systems is monitored.

### Process Architecture

Savvis hosting operations has developed an approach for capturing the dynamic nature of VMs within the virtualized infrastructure. This dynamic infrastructure is captured through the SavvisStation Portal and is available to download as documentation of the virtual infrastructure.

### Utility Storage

The utility storage component is architected to provide information security controls on a virtual SAN (VSAN) infrastructure. The utility storage SSA elements consist of information security, data encryption (transit and at-rest), and security SAN zoning functionality. When using VMware's Consolidated Backup (VCB), all of the VMFs must be presented to a single physical logical unit number (LUN) to be backed up to the VCB server over the SAN. This means that the physical VCB server must be secured since it "sees" all VMFs.

### Technology Architecture

The virtualized infrastructure has all the advantages of the physical from the storage aspect. Savvis provides data integrity, and data-at-rest and in-motion encryption.

### Summary of Secure VM Architecture Protection

In conclusion, despite the benefits of virtualized infrastructure, there are security challenges. Conventional infrastructure security controls designed for dedicated hardware do not map well to virtualized environments. To address these challenges, virtual infrastructure architectures must have well-defined security policies and procedures in place. Additionally, although they will never be fully interoperable with existing dedicated security controls, there has to be some degree of compatibility between the newer security protections specifically designed for virtualized environments and traditional controls.

## WHITE PAPER: Cloud Computing

The table below summarizes the new threat vectors introduced by virtualization environments and how the Savvis Secure VM Architecture addresses these new threats.

Secure VM Architecture	Virtualization Environment Threats					
	VM Escapes	VM Sprawl	VM Hopping	VM Compliance	Inter-VM Visibility	VM Mobility
Policy Management						
Utility Network						
Utility Compute						
Utility Storage						

**Table 1**

### About the Author

Ken Owens is currently the Vice Present of Security and Server Technologies at Savvis Communications. He has made significant contributions in security, server, and virtualization architecture and strategies. Prior to Savvis, Mr. Owens spent 2 years as a Network Security Architect at AG Edwards & Sons, Inc. and Edward Jones Investments respectively. Prior to Edward Jones, Mr. Owens spent 10 years in Architecture and Design of Communications Systems and Components.

### About Savvis

Savvis, Inc. (NASDAQ:SVVS) is an outsourcing provider of managed computing and network infrastructure for IT applications. By outsourcing to Savvis, enterprises can focus on their core business while Savvis ensures the quality of their IT infrastructure. Leading IT organizations around the world have selected Savvis to help them improve their service levels, reduce capital expense and deal with the rising costs of bandwidth, energy, real estate, staff and expertise. As a pioneer in utility computing, Savvis understands and harnesses the latest advances in technology like virtualization, cloud computing and support process automation.

**For more information about Savvis, visit [www.savvis.net](http://www.savvis.net) or call 1.800.SAVVIS.1 (1.800.728.8471).**

EMEA  
Savvis UK Limited  
Tel +44 (0)118 322 6000

ASIA PACIFIC  
Savvis Singapore  
Company Pte Ltd  
Tel +65 6768 8000

JAPAN  
Savvis Communications K.K.  
Tel +81.3.5214.0151