SAVVIS

WHITE PAPER: Cloud Computing

Securing Virtual Compute Infrastructure in the Cloud

Ken Owens
Vice President, Security and Virtualization Platform Technology, Savvis

Table of Contents

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 reduce costs, enterprises have recently implemented virtualization to obtain on-demand access to additional compute resources. This enables enterprises to add processing and storage capacity "on-demand" as required, in order to respond to changing business conditions. Because virtualization allows them to move resources from more-congested to less-congested hosts as required, enterprises also benefit from improved server reliability, which increases application performance. And, consolidating servers through virtualization helps companies achieve "greener" data center operations that are increasingly mandated by corporate sustainability programs.

Despite these benefits, there are also challenges associated with virtualization — 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 will probably never be fully interoperable with existing dedicated security controls, there needs to be some degree of compatibility between newer security protections specifically designed for virtualized environments and traditional controls.

This white paper first discusses the most common security issues that are typically left unaddressed 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 maximize Savvis' Cloud Compute offerings.

New Threats Introduced by Server Virtualization

Most of the new security threats introduced by server virtualization environments arise because virtual machines (VMs) are difficult to secure, both prior to deployment and during day-to-day operations. And, as with any technology implementation, process and people issues also contribute to the challenges of effectively mitigating 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. Therefore, despite the fact that enterprises should experience fewer security issues overall, their operating systems will still be vulnerable.

VM Escapes and VM Hopping

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, VM escapes attack 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, by exploiting vulnerabilities in either the virtual infrastructure or a hypervisor.

Vulnerabilities Associated with Patching Offline Images

Another security vulnerability occurs when enterprises attempt to patch their offline VM images. Current patch management tools cannot accomplish this, making updating signatures and protecting offline VM and VM appliance images from tampering a challenge. 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.

Importance of Network Discovery Capabilities

Another threat arises when there are 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 raise serious security issues.

VMs and Intrusion Prevention Systems

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) that are located in many data center networks*. A virtual IPS solution, integrated with the hypervisor, would prevent direct communication 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 also between guest operating systems, to provide visibility and protection against attacks. The challenge is that signature, filter, and rule updates are necessary for offline VMs. In addition, VMs must be protected from tampering while they are in motion.

Security Policies Should Move with VMs

One of the primary advantages of VMs is that enterprises can move them around the physical environment as required, to obtain additional 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, then 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 a security policy history be maintained on an individual mobile VM?

* Intrusion Prevention Systems are referred to throughout this white paper, as they have grown in usage over the past several years. However, network- and host-based intrusion prevention services may only be available through Savvis as custom offerings. Please contact your Savvis Account Executive for further details.

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 another for the virtual environment. Policies defined by security administrators are not actually being governed by the same administrators in the virtualized environment. Although server administrators are capable of administering server policies, they frequently do not have significant virtualized security training or experience.

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) poses challenges for even the most mature virtualized environments. This is greatly complicated by *VM sprawl*, or the circumstance in which the number of VMs being created grows more quickly than an enterprise's ability to manage them.

People Concerns

As with any new technology, implementing virtualization raises people concerns, as well as the technical and process issues that were outlined in previous sections of this white paper. With virtualization, the primary staffing-related challenge has to do with knowledge of and experience with the environment. For example, current virtualization security and management tools are extremely rudimentary, lack maturity, and security staffs are usually not familiar with them. Indeed, most of the tools that security staffs are most familiar with do not work at all in the VM environment!

As a result, organizations implementing virtualization need to educate their security provisioning and support staff about VM environments. They must also assist server, network, and storage administrators to understand the technology and process challenges that are often associated with virtualized environments.

Architectural Considerations

The challenges outlined above cannot be met by deploying existing technologies or processes. Unfortunately, no single solution exists that will address all of the challenges. Rather, enterprises need to deploy a holistic architectural security strategy that encompasses the technical, process and people aspects of a successful virtualization implementation.

Savvis understands that. We take a different approach to security, by integrating it into all our services rather than 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 its 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 from the beginning, 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, security controls, systems management infrastructure and server management infrastructure have all been integrated.

Enterprises should not relax their compliance and security efforts in virtualized environments, even though controls that exist in the physical server environment may be missing from the virtualized one. That's why a key feature of the 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 Savvis' hosted Compute infrastructure in a secure manner, while maintaining the same policy controls as in physical environments. Savvis' VM architecture provides enterprises with the same degree of visibility and control as they are accustomed to with their dedicated architectures, through its SavvisStation customer portal. This portal is more feature-rich than traditional virtualization management components.

Figure 1

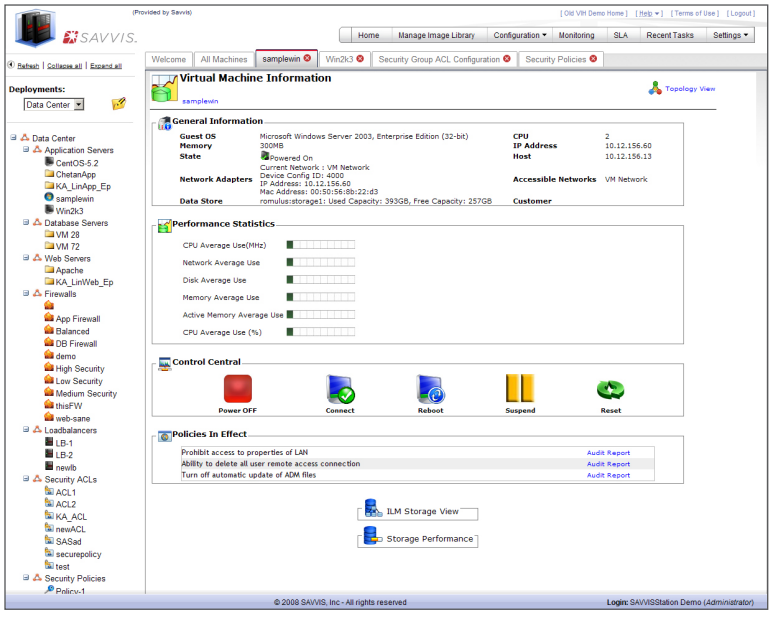


Figure 1 demonstrates the visibility provided by Savvis' VM architecture — including visibility into VMs that are powered off, or those that are in unassigned status in a storage pool.

Figure 2

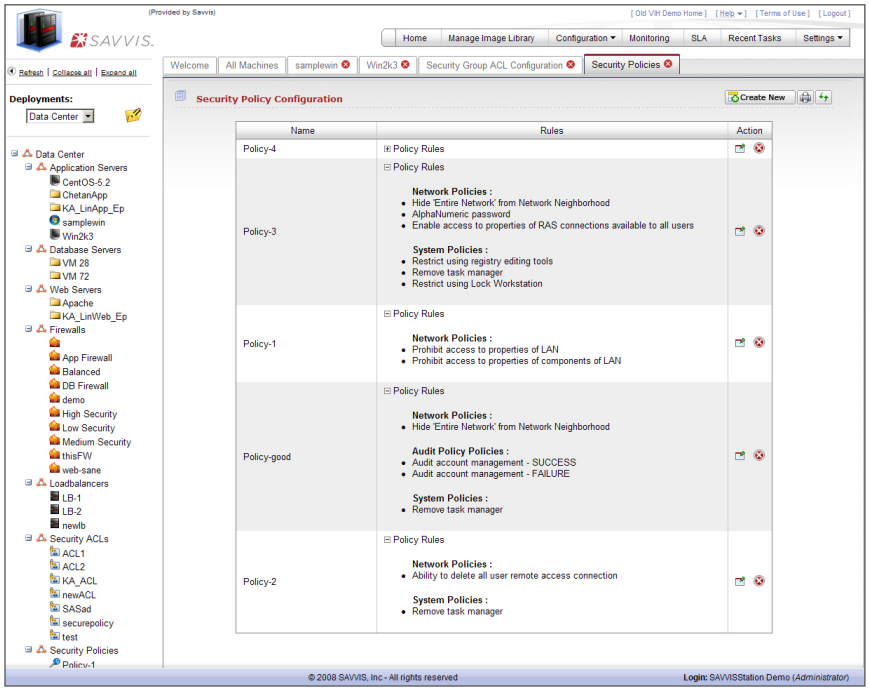
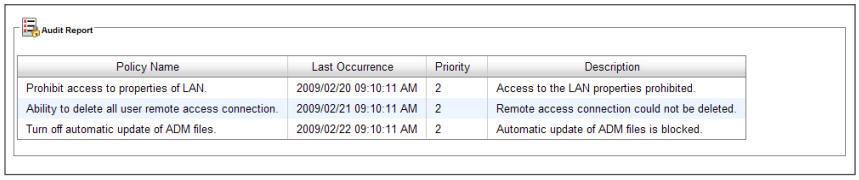


Figure 2 shows the level of policy control that is provided by Savvis' VM architecture. Policies can be selected from defined global policies, or can be modified to better match your organization's desired requirements.

Figure 3



Audit Report

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.

The Savvis VM architecture was developed from the outset to provide audit controls related to VM mobility. A sample audit report is shown in Figure 3.

Defense in Depth

Strategies for ensuring perimeter security have evolved significantly over the past several 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 inter-VM communications. This is because when one VM is compromised, then all of the other VMs that are part of the virtual network can be compromised, without being detected. To ensure that each layer of the infrastructure possesses equivalent security controls, Savvis' VM architecture provides layered security components in both physical and virtual environments.

By providing 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 Savvis' VM architecture is that enterprises can move these security policies, and the data collected about them, along with the VMs. This allows them to consistently enforce security policies.

In addition, by design, the Savvis 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 does not become compromised.

Patch Management

One of the biggest security challenges related to security management within 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 that are available in the virtual world. A number of key questions have yet to be 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 pre-defined schedule, or require a VM to power on only in a demilitarized zone (DMZ) that can remediate, prior to releasing the VM to production. Another solution is not to permit offline VMs into the infrastructure. But, these solutions limit the availability of virtual servers and can hinder organizational agility.

Savvis' VM architecture offers a policy control service that can provide some offline patching capabilities. It integrates with an enterprise's existing server management platform to ensure consistent policies are adhered to in both physical and virtual environments. The 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 the appropriate manner.

Vulnerability and Configuration Management
Virtualized security architectures must include sufficient vulnerability and configuration management capabilities. Savvis' 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 of this can be accomplished without running the VM itself, as the architecture provides a mechanism to perform what-if analyses to check the configuration state and potential vulnerabilities associated with starting the VM on a target system.

Additionally, Savvis' VM architecture is completely integrated with Savvis' Threat Management Service architecture, to provide end-to-end vulnerability and threat management correlation and resulting policy configurations.

Identity and Access Management
Auditors have expressed a great deal of concern about VM environments' inability to control user-access. Savvis' VM architecture defines a VM identity that ties each VM to an identity within Savvis' managed infrastructure. Based upon this identity, Savvis is able to assign user, role and privilege access within the virtualized 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' VM architecture can prevent the VM from being cloned or copied, by utilizing a combination of VM identity and server configuration management policies.

A Virtual Security Architecture

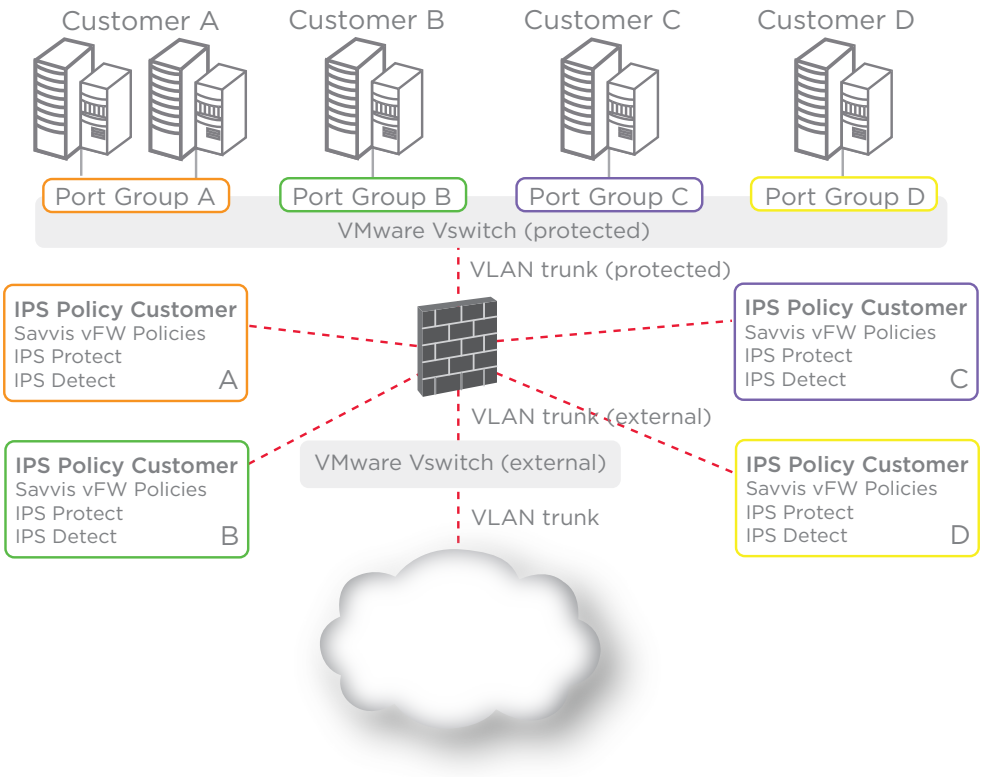
A virtual security architecture must defend enterprises against the new threats introduced by virtualization, while maintaining performance and organizational agility. Savvis' VM architecture is comprised of two distinct sub-architectures:

- VM Policy Services Architecture
- VM Threat Management Services Architecture

Savvis' VM architecture is a sub-set of Savvis' Security Architecture (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, are defined in greater detail below. When reviewing the diagram, please note that the acronym "vFW" refers to Savvis' virtual firewall capabilities.

The Savvis VM architecture is displayed in Figure 4.

Figure 4*



*IPS/IDS is planned architecture for Savvis' Project Spirit cloud enterprise release. Please refer to Savvis' press release dated 9/1/2009 for further details about Project Spirit.

Policy Services Architecture	Threat Management Services Architecture
Customer-defined policy management	Secure, virtualized infrastructure that provides protection from VM escape and VM hopping attacks
Security policy reporting	Provides inter-VM visibility and blocking through VIPs (virtualized IP addresses)
VM identity and access policies	Deep packet inspection through vFW (virtual firewalls)
Monitoring of guest Operating System (O/S) configuration policies	Network access control
Enforcement of mobility policies	
Ability to 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.

The policy management service elements consist of:

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

Many of the services outlined above can be provided by Savvis, either as Managed Security Services or as Professional Services. Please contact your Savvis Account Executive for further details.

The impact of virtualization on the policy management services component is addressed by the technology and process element architectures that are 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 permits Savvis to manage access control policies on the VM — where it can start up, what users are authorized to access it, and even on which systems it can run.

The security agility element can provide much-needed controls and policies to improve the security of mobile VMs. In addition to monitoring the VMs, the security agility service delivers VM policy reports. By defining VM identity and access policies with an enterprise's security control and audit reporting requirements, 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 to stop or suspend — VMs, and the ability to view and start VMs, but not to 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, customized Intrusion Detection System (IDS) 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 that are 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 in a virtualized infrastructure.

Process Architecture

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

Utility Compute

The utility compute component is architected to provide security hardening of layered security attributes that are available for grid, high-performance and virtualized computing infrastructures. In the future, the utility compute elements of the SSA are expected to consist of multiple Web-based (XML/SOA) firewalls, VM IPS and Host-based Intrusion Prevention System (HIPS) Service functionality. As of September 2009, Savvis currently offers a Web Application Firewall (WAF) Service that is powered by Imperva's SecureSphere technology.

Technology Architecture

The forthcoming VM IPS element is expected to consist of inline virtualized intrusion prevention services. The patch management element provides patch management of offline images, and the ability to manage policies associated with 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 team 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 for download as documentation of the virtual infrastructure.

Utility Storage

The utility storage component is architected to address certain information security controls on a virtual SAN (VSAN) infrastructure. Savvis' current and planned utility storage SSA elements consist of information security 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), in order 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

From a data storage perspective, a virtualized infrastructure has similar benefits as those provided by a physical infrastructure. Savvis' current and planned storage capabilities will include data integrity and data-at-rest and data in-transit encryption.

Summary of Savvis VM Architecture Protection

In conclusion, despite the significant benefits provided by virtualized infrastructures, organizations need to be mindful that such environments also pose security challenges. Conventional infrastructure security controls designed for dedicated hardware simply do not map well to virtualized environments. To address these challenges, virtualized architectures must have well-defined security policies and procedures in place. Additionally, although virtualized security protection methodologies will never be fully interoperable with existing dedicated security controls, there needs to be some degree of compatibility between those specially designed for virtualized environments and traditional controls.

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

Table 1

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

About the Author

Ken Owens is currently Vice President of Security and Virtualization Platform Technology at Savvis. 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 working at 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 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