

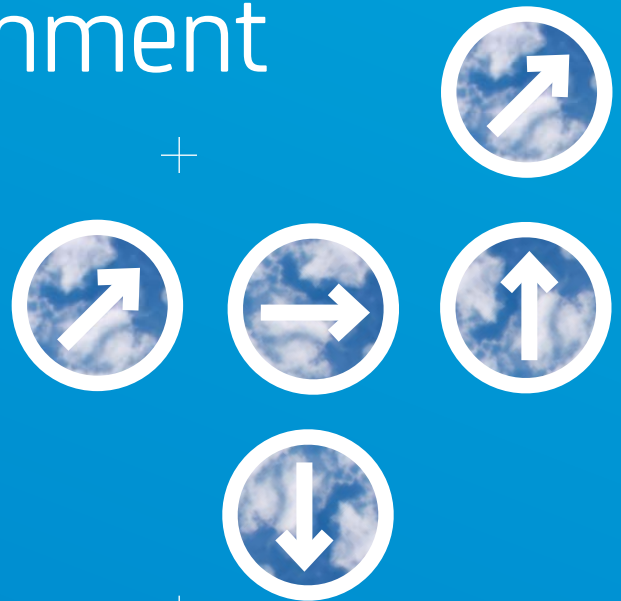


Executive Brief




The Building Blocks for a Secure Virtualized Environment

As virtualization moves into the mainstream, IT leaders need to know that their IT environments will remain secure.

This Executive Brief will help IT leaders understand what security risks their companies may be exposed to in a virtualized environment, how to manage them, and ways they can reduce them.



Inside:

-  Nemertes: How To Build a Secure Virtual Environment
-  Why Is Virtual Security Such a Problem?
-  Protecting the Virtual Environment
-  Looking Ahead: Embrace the Cloud
-  Additional Reading

How To Build a Secure Virtual Environment

By John E. Burke
Principal Research Analyst, Nemertes Research

Everyone is virtualizing their data centers. Already, 97% use server virtualization, according to Nemertes' 2010 benchmark study. Approximately 13% of data centers are fully virtualized. These data centers are now running, on average, 78% of enterprise applications on virtual servers. SMBs in this group are running 64% of enterprise applications on virtual servers; large enterprises, 99%. In those data centers still rolling out virtualization, 47% of enterprise applications run on virtual servers. Half of organizations already have some virtual desktops — which pulls desktop operating systems and security problems into the data center.

Virtualizing makes the organization more agile, but it shakes up security. Hypervisors introduce little risk to the environment, but the ways IT uses them does. Servers that had been physically segregated onto separate LANs in a data center often find themselves on the same host server, with only whatever level of segregation the hypervisor can enforce. Systems that may have had a firewall and Intrusion Detection System (IDS) or Intrusion Prevention

System (IPS) between them in the physical network don't in the virtual space. Huge amounts of network traffic occur where IT has little visibility and a different — often lesser — level of control than it used to.

To secure the hybrid of physical and virtual systems, IT needs to get back to basics: assess the security and risk profile of the new environment; deploy defense and visibility in depth; and bring management of disparate security tools and layers together.






Assess security profile of virtualizing environment.

Fewer than 36% of organizations in Nemertes' benchmark research have conducted a formal assessment of virtualization's impact on their security or compliance profile. This is a problem! Servers sharing hardware and a hypervisor environment can have significant compliance implications, especially if a compliance regime requires separation of administrative access and duties, or segmentation of application tiers. Virtual server administrators having access to

virtual network configuration, for example, makes vulnerability through misconfiguration a real possibility, too.

Virtual infrastructure is far more dynamic than physical infrastructure: physical servers rarely move from rack to rack, let alone among data centers, but virtual machines can do it several times a day. Traditional physical segmentation and appliances have a hard time coping with this dynamism, either because rules can't be set up that are sufficiently flexible, or because they simply require that a server be in a certain place, hanging off a specific set of switch ports. Because physical location becomes a dynamic variable in a virtualized data center, the extent to which security depends on physical location is a key consideration in assessing security in a virtual infrastructure.

Equally important to the changes in the environment are the changes virtualization brings to process and management. Virtualization speeds IT up — stripping out 80% or more of the time it takes to provision a

-  [Nemertes: How To Build a Secure Virtual Environment](#)
-  [Why Is Virtual Security Such a Problem?](#)
-  [Protecting the Virtual Environment](#)
-  [Looking Ahead: Embrace the Cloud](#)
-  [Additional Reading](#)

server, for example — and that means security has to speed up too. Lots of security is embedded in provisioning checklists — and in administrators' heads. Take days or weeks out of the process and the chance that items get forgotten or checked off the list mistakenly increases dramatically. So, a thorough security assessment of the virtualizing environment requires examining process as much as environment.

Defense and visibility in depth. Once IT has taken a fresh and honest look at the new security landscape in their data center, it needs to remedy the introduction of new, unacceptable levels of risk. They may approach this via direct controls — firewalls, IPS systems — or compensating controls, such as increased visibility and reporting on network traffic.

Direct controls can include new security tools within the virtual environment, such as virtual firewall appliances. Nemertes finds fewer than 4% of organizations adopting such specialist tools (with just over 15% evaluating them).

In the long run, whether through the layering of third-party tools or by waiting for hypervisor vendors to implement sufficient security functionality themselves, every virtualized data center needs to push a high-visibility, defense-in-depth

strategy into their virtual environment.

Defense in depth doesn't just mean digging into the virtual environment; it also means increasing emphasis on higher-level security constructs: identity and organizational role. Identity management and role-based access control make *who an entity is* (whether it is a person, or a system, or a software component) and *what its role in the organization requires it to do* the basis of both access management and information protection. Protecting data and systems by focusing on identity and role helps insulate access management from the dynamism of the virtual environment. When identity is validated by something other than location, say a security token rather than an IP address or an access-switch port number, then location changes have no effect on access control.






Integrating security. With plans for controls in mind, IT needs to ensure that there will be no gap between physical and virtual security, either in setting policy or executing on it. Establishing an environment in which there is no automated synchronization of security settings between physical and virtual environments, or no consolidation of logs across both, begs for security holes to develop as virtual infrastructure moves at the speed of virtualization and the rest of the infrastructure does

not. This makes it increasingly important to deploy tools that can integrate management and monitoring of both physical and virtual environments, and both appliance-based and host-based versions of the same tools; for example coordinating policy settings on host-based as well as physical and virtual firewall or IPS appliances.

And this is the run up to cloud! With a physical/virtual security environment that deploys defense and visibility in depth without hobbling the dynamism and resilience of the virtual environment, IT has established a firm foundation for extending operations into the cloud infrastructure. The same kinds of tools, policies, and processes that support virtual infrastructure in-house can, with the addition of federation, extend to support it as workloads flow to the cloud.

This research report represents the existing findings and opinions of Nemertes Research and is free of sponsorship of any kind.

About Nemertes Research: Nemertes Research is a research-advisory firm that specializes in analyzing and quantifying the business value of emerging technologies. You can learn more about Nemertes Research at our Website, www.nemertes.com, or contact us directly at research@nemertes.com.

-  Nemertes:
How To Build a Secure Virtual Environment
-  Why Is Virtual Security Such a Problem?
-  Protecting the Virtual Environment
-  Looking Ahead: Embrace the Cloud
-  Additional Reading

Why Is Virtual Security Such a Problem?

IT's increased use of virtualization technology is due to the benefits of streamlined operations and reduced operating costs. But in a virtual environment, the security challenges multiply rapidly and introduce new risks.

Where an organization might have had a single application server, they could see that quickly evolve to 30 servers. How can security be maintained, not only on a physical machine, but also on the virtual machines it hosts, and the applications running on those virtual machines? And how can an organization control and manage this from a central location?

As an example, a Fortune 500 company takes up to six months to deliver a server to their internal customer, which is five months and three weeks too long for them to remain competitive. By using virtualization technology, they expect to reduce that interval to five business days.

From an operating cost perspective, by using virtualization technology, IT can approach 100% utilization of a physical server. In return, they may reduce physical space requirements, which, in turn, may also reduce their real estate, personnel, bandwidth, and Heating, Ventilating, and Air Conditioning (HVAC) costs.

Physical security is well established.

Over the past 50 years, security for physical IT operations has become well established. Whether the security involves

controlling physical access to a server (e.g., rack-mounted server cages) or identity management software, rules, processes, and best practices have been established.

Security software has evolved to provide IT with the right tools to manage the physical environment. In addition to identity management, application security, access control, information control, user activity logging, and reporting are all solutions being used effectively today.

Virtualization technologies can be more difficult to secure than physical machines. Regardless of whether it is a physical or virtual environment, the need for complete security management remains. Meeting compliance regulations, managing and governing identities, controlling access, as well as finding, classifying, and controlling how information is used, are the biggest challenges facing IT as they migrate to virtual environments.

Virtualization technologies enable the execution of multiple operating system instances, or virtual machines (VMs), on the same physical piece of hardware. Each VM functions as if it were its own physical machine with a dedicated operating







PODCAST:

A Practical Approach to Virtualization Security

Are the security procedures your company has instituted for a physical server environment effective and relevant for a virtual server environment? How can you make sure the information and workloads are protected in a virtual environment? Or that they are meeting compliance requirements? Learn the answers to these questions and more during a conversation with Shirief Nosseir, Europe, Middle East, Africa Product Marketing Director for Security Management at CA Technologies. [LISTEN](#)

In the physical server environment, native operating system security does not provide protection for mission-critical data and resources at the level needed to meet regulatory compliance and security best practices, and this carries over to the virtualization environment.

-  Nemertes: How To Build a Secure Virtual Environment
-  Why Is Virtual Security Such a Problem?
-  Protecting the Virtual Environment
-  Looking Ahead: Embrace the Cloud
-  Additional Reading

Why Is Virtual Security Such a Problem? *Continued*

system and hosted applications. The layer within the virtualization platform that enables hardware resource sharing among VMs is called the “hypervisor.”

When we want to identify the risks of virtualization, we first need to understand how virtualization is different from traditional physical environments. In the physical server environment, native operating system security does not provide protection for mission-critical data and resources at the level needed to meet regulatory compliance and security best practices, and this carries over to the virtualization environment. The virtualization host becomes more critical as it hosts many virtual machines—not only one. The hypervisor serves as a single management point to all VM images and control over many critical services, creating a vulnerability leverage point. A person with hypervisor access is analogous to a root user in the UNIX world; this person can do anything to any of the hosted machines.

Compromising the hypervisor to download an image or introduce a rogue VM is equivalent to bypassing physical security to break into a server room in order to steal a machine or introduce an unauthorized machine to the data center. Virtualization management applications can be bypassed and the hosting operating system or virtualization console can be accessed directly by privileged users.

We used to have servers stacked away in

our server room with tight physical controls in place to control access to the boxes. In a virtual environment, servers are files that can be copied from the host. Copying a server image is equivalent to stealing a server from the server room. Furthermore, machine memory can be accessed from the hypervisor, compromising transmitted information like passwords and encryption keys. So, safeguarding access to the virtualization host—even remote access—is critical. The modern virtual data center is highly distributed, unlike the traditional mainframe. Risks that were previously mitigated using physical security must now be handled by IT security.

Managing roles, identities, and applications. If identities are not well managed in the physical world, then attempting to implement a virtual environment will exacerbate the identity and access problems that exist today. Using software to clearly define and manage users and roles is what many companies do today. This then coordinates with an identity management solution to confirm that users are only granted the appropriate privileges. If not managed properly, uncontrolled, overprivileged users will be able to wreak havoc on a greater number of systems and applications in a virtual environment.

On the other side of the security spectrum is the need to manage secure access to applications, by users as well as other applications or services. In a virtualized environment, application servers will

POLL

What are your primary inhibitors to securing virtual environments?






Inhibitors

- Lack of expertise & skills
- Budget & upfront cost of implementation
- Low priority on the management’s agenda
- Lack of awareness in your organization of the inherent risks
- Complexity of managing security across virtual environments & platforms
- Lack of relevant processes, policies & standards within your organization
- Immaturity of security & management tools in the market
- Vendors lack licensing & deployment options optimized for virtual environments

Select all that apply

VOTE

Gartner found that 60% of virtualized servers will be less secure than their physical counterparts through 2012.

-  [Nemertes: How To Build a Secure Virtual Environment](#)
-  [Why Is Virtual Security Such a Problem?](#)
-  [Protecting the Virtual Environment](#)
-  [Looking Ahead: Embrace the Cloud](#)
-  [Additional Reading](#)

Why Is Virtual Security Such a Problem? *Continued*

come online and go offline as computing demands ebb and flow. A scalable access management platform to provide proper fine-grained access controls needs to be in place before virtualization of many applications can take place. This enables organizations to leverage a reliable and secure platform for both the physical and virtual environments.

Controlling privileged users. Normal users are identified and controlled by the operating system and application security. They may make mistakes or attempt misuse; however, provided the controls are correctly set, they should not be able to breach confidentiality or damage the system.

The privileged user, however, has elevated privileges on the servers. The privileged user's access is not controlled by the native operating system security at the level needed to meet regulatory compliance and security best practices, and his/her username and/or password is typically shared between administrators, making him/her mostly anonymous.

Virtualization makes the problem worse. The administrator not only has leverage over the physical host, but also all of the virtual sessions running on it. He/She can also have access to sensitive data and have an impact on business continuity. Without an independent access control solution, multiple privileged users in various roles have the ability to interact with numerous

WEBCAST

Empowering Transformation: Managing the Risks of Virtualization








With major advances in virtualization and cloud computing coupled with current economic conditions, IT organizations are adopting and adapting to more efficient, cost effective and business friendly platforms to deliver more value to the business. The CA Virtualization Webcast series "Empowering IT Transformation" delves into the risks and rewards of today's IT transformation into adopting server virtualization and cloud. Listen as CA Technologies' Chris Wraight and Forrester's Andras Cser discuss how to keep the virtualization risks in-check.

components of a virtualization deployment. This inadequately regulated access to the hypervisor presents the potential for significant damage to the enterprise through the compromise of valuable information and disruption of critical services. VM images can be copied, along with the data and applications that they hold. These images can be brought back online on an unsecured network, making it easier for an intruder to access the contents managed within the copied image.

A well-meaning developer at a large insurance company made a clone of a production VM and launched it in a quality assurance (QA) environment. The company had no controls on access, so the developer was allowed free access to QA, Development, and Production environments. When

he turned on the copy of the system, the machine behaved as though it was in production. The developer ran some claims scenarios in order to test functionality, and didn't realize that the system was actually cutting checks and kicking off the process to mail the checks to customers. One customer received two checks for a claim that was already in process and called to ask about which one should be cashed; this was the way the company found out what was occurring. This is the nightmare scenario for many IT organizations.

Data sprawl grows rapidly. As virtualized servers grow, so too does the amount of sensitive company data residing on them. Personal medical files, proprietary product plans, employee records, and credit card data is information that needs

-  [Nemertes:
How To Build a Secure Virtual Environment](#)
-  [Why Is Virtual Security Such a Problem?](#)
-  [Protecting the Virtual Environment](#)
-  [Looking Ahead: Embrace the Cloud](#)
-  [Additional Reading](#)

Why Is Virtual Security Such a Problem? *Continued*

to be located and prevented from leaving the organization. How can an organization keep track of this information, especially if VMs may come online and go offline?

Inadequate auditing hampers compliance. Given the leverage the virtualization platform has on the stability of the entire data center and on the integrity of the data it manages, it must be viewed as critical infrastructure. As a result, the virtualization platform is subject to tight compliance requirements. Organizations must track the interaction that each user has with the virtualization platform and within each of the VMs it hosts. However, native audit capabilities provided by these environments are too coarse to be effective and are vulnerable to tampering and to snapshot manipulation.

Auditors, until lately, have not been virtual-

ization savvy, and virtualization audit issues haven't yet been regularly flagged. But this is changing, as seen by the recent updates to various common regulations such as payment card industry. Access to the hosting operating system must be tracked and audited to prove controls have maintained its integrity and effectiveness. Similarly, within each VM, access gained to each guest operating system is subject to the same regulatory compliance requirements.

Content-Aware Identity & Access Management (IAM) solutions. As security perimeters continue to blur and virtual workloads become more mobile, it is clear that security needs to be applied to identities all the way to the data throughout its lifecycle, rather than just to network assets. This makes it essential for virtualization and cloud computing efforts to adopt an identity-centric

and content-aware security strategy from the very start. Content-aware IAM helps you strengthen and automate your security controls, because it enables you to control user identities, their access, and their information usage. While traditional IAM stops at the point of access of applications and systems, content-aware IAM goes beyond this by providing management and control starting at the user all the way to the information and how it is used. This granular control helps you prevent misuse of your data, including improper disclosure or theft from the organization — improving your compliance posture and protecting your critical information assets across physical, virtual, and cloud environments.

To learn more and to download the entire white paper, “Content-Aware Identity & Access Management in a Virtual Environment,” please [click here](#). ■

The screenshot shows a video player interface. The main content is a presentation slide with the following text:

- Opportunity Versus Risk: What is the Right Balance When Adopting Virtualization**
- Transforming IT Management.
- Opportunity Versus Risk: What is the Right Balance When Adopting Virtualization?**
- Featuring:**
 - Neil MacDonald**
VP & Gartner Fellow
 - Gijo Mathew**
VP Security Management, CA
- Featured Analyst Firm**
Gartner
- The info contained within all 2016 documents are online. Copyright © 2016 Gartner, Inc. All rights reserved. All confidential and proprietary information has been removed and any other information is subject to change without notice. Released June 2016. Mobile Analytics/Insight. Issued by Security Management. AccelCast

The video player controls at the bottom show a play button, a progress bar at 0:16 / 30:32, and other standard controls.

Opportunity vs. Risk: What is the Right Balance When Adopting Virtualization?

Join Neil MacDonald, Vice President and Research Fellow at analyst firm Gartner, Inc. as he looks at the opportunities and associated risks — both for security and service — in adopting virtualization. Gijo Mathew, Vice President of Security Management at CA Technologies talks about how effective management approaches can provide a catalyst to achieving IT's business and strategic goals by effectively harnessing these technologies. [WATCH](#)

- Nemertes: How To Build a Secure Virtual Environment
- Why Is Virtual Security Such a Problem?
- Protecting the Virtual Environment
- Looking Ahead: Embrace the Cloud
- Additional Reading

Protecting the Virtual Environment

CA Access Control (AC) provides the critical layer of protection needed to effectively protect virtualization platforms. AC operates independently, both at the application level and at the operating system kernel level, without interfering with the kernel itself. By securing console access to the hypervisor, AC protects mission-critical information and services running in the virtual data center. It protects virtualization deployments at multiple levels: operating systems hosting a hypervisor, operating systems implementing operating system-based virtualization, privileged partitions managing hypervisor-based virtualization and the critical resources in virtual machines (VMs) running on all of the

above. Support of a wide range of operating systems makes AC ideal for protecting VMs, especially in a heterogeneous operating system environment. AC also allows you to protect privileged users across IT environments beyond the virtualization host itself—on databases, network devices, and applications. It also helps simplify user management by consolidating the user management under a single authoritative source across all operating systems.

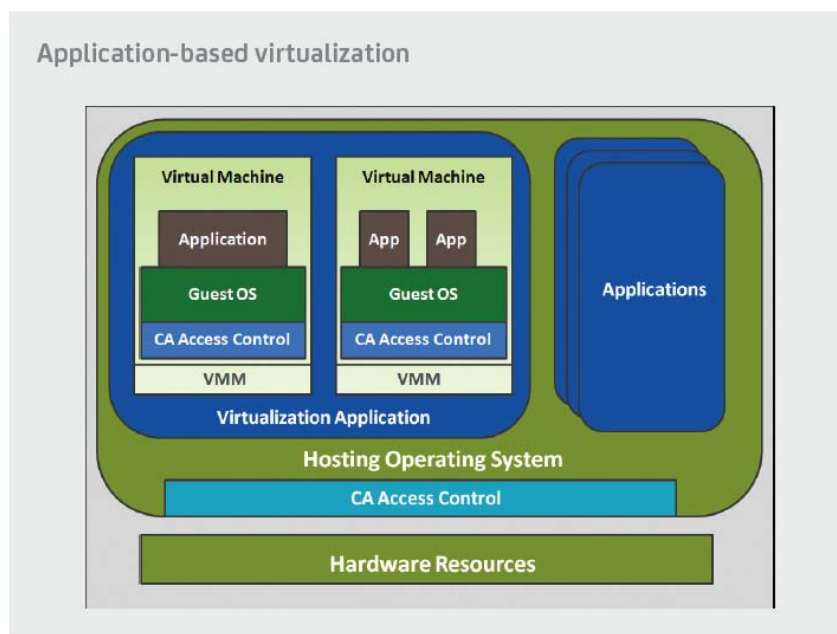
To learn more and to download the entire white paper, “Securing Virtualized Environments and Accelerating Cloud Computing,” please [click here](#). ■

POLL

Will your organization leverage virtualization to deliver private cloud computing services?
(select one option)

- Yes, we already do today
- Yes, expected before end of 2011
- Yes, expected before end of 2012
- No, we need to ensure our virtualization processes are mature enough first
- No, we feel that private clouds are not yet trustworthy/mature enough
- No, we do not see much value yet in private clouds

VOTE



- [➤ Nemertes: How To Build a Secure Virtual Environment](#)
- [➤ Why Is Virtual Security Such a Problem?](#)
- [➤ Protecting the Virtual Environment](#)
- [➤ Looking Ahead: Embrace the Cloud](#)
- [➤ Additional Reading](#)

Looking Ahead: Embrace the Cloud in a Managed and Secure Fashion

Just when organizations thought it was safe to coast forward incrementally with their Identity and Access Management (IAM) strategy, along came the cloud with a new set of business opportunities and challenges to disrupt the status quo.

The cloud is a disruptive, business-driven IT phenomenon created in response to the economic realities and mounting pressures to reduce costs and increase efficiency and agility with computing. It introduces new (yet familiar) models for consumption and delivery of applications that have a democratizing effect: applications and other IT services that were once only available to companies with deep pockets and large IT shops are now accessible to all. . . and for seemingly much less cost.

While the cloud addresses many problems, however, it also brings up many new ones. As a visionary in the area of IT and IT management, CA Technologies has spent years anticipating these new dynamics. We have been carefully shaping our product strategy accordingly and continue to execute on it. As an IAM market leader, we are helping drive industry activity that will establish standards and best practices to instill user and enterprise trust.

One thing that is clear is that identity, and the management and controls dependent on it, are absolutely central to the secure

adoption of cloud services. The goal of this paper is to share CA's experiences and understanding of the challenges, and to provide the reader with an overview of our strategy and vision for Identity and Access Management for the cloud.

Target audience

Traditionally, IAM challenges and the products that address them have been focused on large enterprises and governments that contain large, dedicated IT infrastructures and lots of applications and users. These organizations have recognized firsthand the challenges of giving and controlling users' access to applications in large, heterogeneous environments. However, with the cloud, the audience that needs to seriously consider IAM expands to other communities, including smaller organizations, cloud service providers, and government entities.

Small organizations now face IAM challenges too as they move from the homogeneous Microsoft Active-Directory-centric identity world that they currently inhabit to one where their IT services will come from a varied and heterogeneous world of the cloud.

Cloud service providers are also trying to take advantage of the move to the cloud to deliver externally identity-based and enabled services and internally to secure virtualized and multi-tenant systems.

POLL






What is your most important challenge/concern related to securing your virtual environments?

- Maintaining compliance with regulatory & audit requirements
- Preventing sensitive data from creeping into less secure virtual environments
- Maximizing automation by tightly integrating security with infrastructure & service management
- Managing the far-reaching privileges introduced by hypervisors & enforcing separation of duties for administrative tasks
- Controlling virtual server sprawl & simplifying change & configuration management

VOTE

49% of organizations use cloud computing applications that are not thoroughly vetted for security risks.

PONEMON INSTITUTE SURVEY, MAY 2010

-  Nemertes: How To Build a Secure Virtual Environment
-  Why Is Virtual Security Such a Problem?
-  Protecting the Virtual Environment
-  Looking Ahead: Embrace the Cloud
-  Additional Reading

Looking Ahead: Embrace the Cloud in a Managed and Secure Fashion *Continued*

Around the world, governments are providing identity cards, which work equally well online as in the physical world. Identity plays a big part in that too.

Organizations (large and small), cloud service providers, and governments are thus the target audiences of this paper. Each type of organization is asking questions related to identity and the cloud for:

- **Large organizations.** How to extend existing IAM systems to manage users and their access to cloud-based applications and services
- **Smaller organizations.** How to leverage a multitude of cloud services without encumbering your users and losing control of your organization

- **Cloud service providers.** How to provide your IT services in a way that is highly efficient and meets the security needs of your enterprise and consumers.

Please note that this paper is not intended as a primer for IAM (authentication, authorization, SSO, etc.) or cloud concepts. Such introductory concepts are best pulled from other sources.

To learn more and to download the entire white paper, "Identity and Access Management for the Cloud: CA's Strategy and Vision," please [click here](#). ■

➔ ADDITIONAL READING

WHITE PAPER:

[IDC White Paper: Identity and Access Management for Approaching Clouds](#)

PONEMAN INSTITUTE RESEARCH REPORT:

[Security of Cloud Computing Users—A Study of Practitioners in the US & Europe](#)

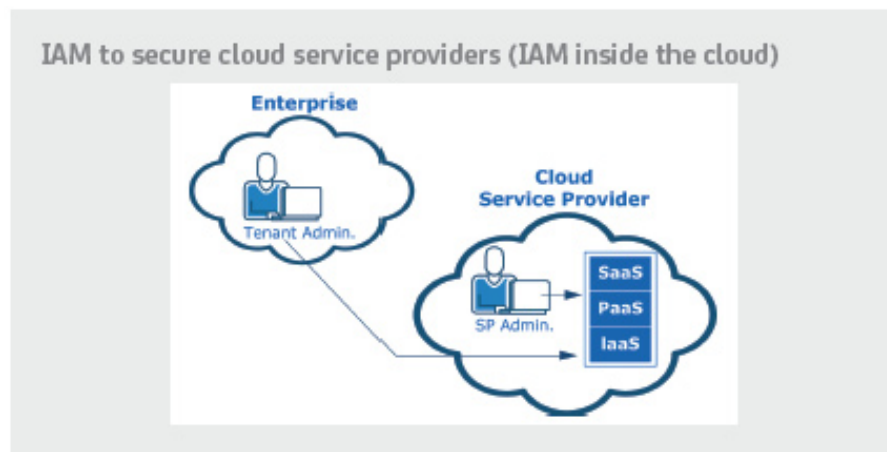
WEBCAST:

[Identity as Security Glue for the Cloud](#)

While discussions of cloud security often focus on threat and data privacy issues, there is another dimension of cloud security that deserves attention: identity and access management (IAM). Join Matthew Gardiner, Director of Security Management at CA Technologies, as he provides a framework for thinking about identity and how it relates to both the different modes in the cloud as well as the consumption and use of the cloud.

WHITE PAPER:

[CA Point of View: Content Aware Identity and Access Management](#)



68% of respondents said that their organization's security leaders are not the most responsible for securing their organization's safe use of cloud computing resources.

PONEMON INSTITUTE SURVEY, MAY 2010

- ➔ Nemertes: How To Build a Secure Virtual Environment
- ➔ Why Is Virtual Security Such a Problem?
- ➔ Protecting the Virtual Environment
- ➔ Looking Ahead: Embrace the Cloud
- ➔ Additional Reading