IDC Analyze the Future

I D C  T E C H N O L O G Y  S P O T L I G H T

# Rethinking Security for Virtual Environments

*April 2012*

Adapted from *Market Analysis Perspective: Enterprise Virtualization Software – Mainstream Adoption of Virtualization to Enable Cloud and Mobility, 2011 and Beyond,* by Gary Chen, IDC #227532

Sponsored by Kaspersky Lab

*This Technology Spotlight will explore the benefits of using an agentless, hypervisor-based approach to endpoint security and discusses the role that Kaspersky Security for Virtualization can help play in enhancing security on the VMware platform.*

## Introduction

The first phase of virtualization focused on test and development workload consolidation supported by multiple virtual machines (VMs) per physical server. That activity began in earnest in 2005 and has accelerated with the continuing maturation of virtualization technology.

By 2008, the second generation, Virtualization 2.0, was underway, and the focus was consolidating production applications. The industry also saw the introduction of dynamic functionality such as live migration and extended virtualization use cases such as high availability. Usage cases have also spread to desktop with virtual desktop infrastructure (VDI) technology, which consolidates desktops onto servers running as VMs.

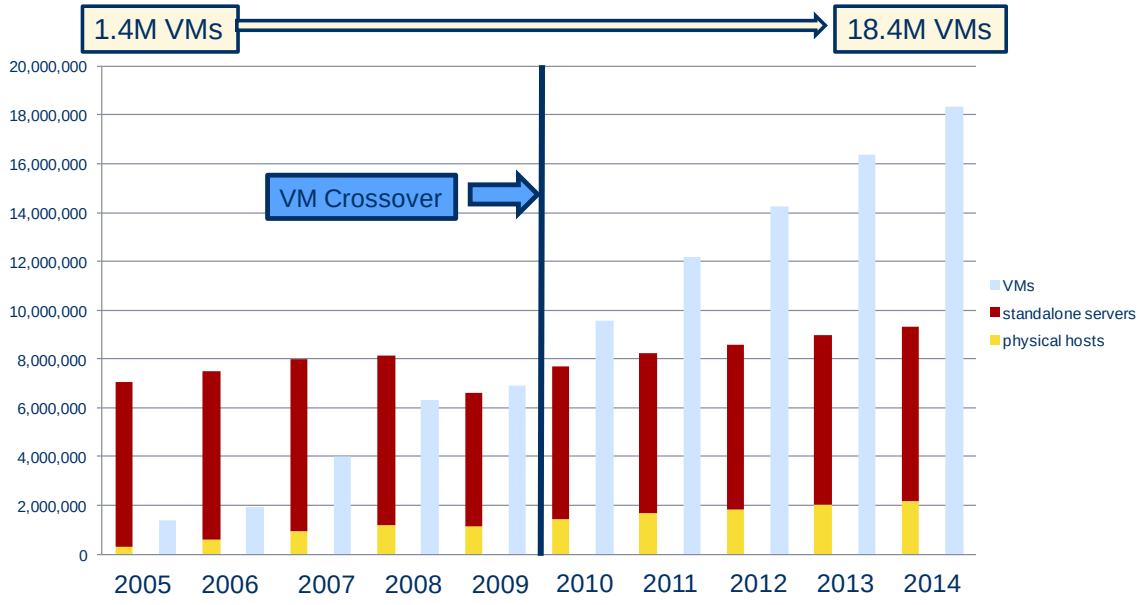
Today, IT organizations are transitioning to a third era, Virtualization 3.0, which is taking on cloud-like attributes for highly virtualized and automatically managed internal deployments. Virtualization 3.0 expands virtualization beyond just hypervisors and servers. Server virtualization has been the catalyst for the 3.0 era, and it has driven transformation into every aspect of the datacenter, such as storage, networking, security, and management. Successful virtualization deployments today require a holistic approach and an end-to-end view of virtualization.

Virtualization today is clearly the new norm. IDC data shows that virtualization makes up the majority of today's server deployments:

- Virtualization has already eclipsed physical in new server shipments, with the VM crossover point taking place at the end of 2009. By 2014, IDC forecasts that VMs will out-ship physical servers more than 2:1 (see Figure 1).
- From a workload perspective, at the end of 2010, more than half of all installed workloads were virtualized. IDC forecasts that, by 2013, more than two-thirds of installed workloads will be virtual.
- More than 75% of virtualization customers have a virtualization-first policy in place.

**Figure 1**

Server Virtualization Shipment Forecast, 2005–2014




Source: Server Virtualization MCS, 2010

## Virtualization Impacts Every Datacenter Decision

Every area of datacenter IT has been impacted in some way by virtualization and has fundamentally changed the paradigm of the underlying compute layer:

- Consolidation of workloads means that workloads share resources, but this introduces prioritization and service-level management issues.
- VMs are software objects that can easily be created and destroyed, which enables advanced features like elastic scaling, but they also introduce VM sprawl issues if IT processes are not addressed.
- VMs can also be dynamically moved from server to server and from storage device to storage device on the fly without incurring downtime. This creates a dynamic environment for which many current solutions simply were not designed.
- VMs are simply stored as files on a disk instead of being installed bare-metal on a disk/server. This means that VMs can be managed easily using normal file management tools, but this also means that VMs can sit around on a disk indefinitely offline and become progressively out of date with software patches and updates.
- Virtualized desktops completely change the desktop paradigm computing model. Desktops are now running on datacenter servers and storage as VMs, which are consolidated on a hypervisor. Endpoints only need to have the limited functionality of a thin client to connect to the server-based VM. Desktops deployed in this fashion will suffer from the same issues listed above that affect any server-based image but also introduce new issues, as desktop workload patterns are very different from server workload patterns – for example, dealing with daily morning 'boot storms' as employees start up their desktops at the same time.

The biggest areas impacted by virtualization initially were around storage and systems management. As we move more into the 3.0 era of cloud, other disciplines are being affected as well, such as networking and security.

## Security Concerns in a Virtual World

Virtualization benefits can overshadow security concerns. The consolidation of servers can provide a single point of risk relative to malicious software. Given the scale of these environments, it is critical that virtualized security integrates seamlessly with management for servers and endpoints.

IDC believes that, if you cannot see it, you cannot manage it and you cannot secure it. Enterprises should consider a single unified management and security platform across their entire virtual, physical, and mobile environments for risk management and consolidated administration.

At a deeper level, the fundamental concept change introduced by virtualization has several of the following significant effects on security when you consider the classic approach of agent-based malware protection:

- Due to the consolidation effect of virtualization, this leads to duplication of the agent in each VM on the host server, resulting in inefficient use of resources.
- Since each agent is running independently, there is no coordination among them. This can lead to scenarios in which multiple agents on a host server each begin to kick off signature updates or antivirus (AV) scans simultaneously, starving resources and affecting the operation of other VMs on the host. These are often called 'AV storms'.
- VMs are typically provisioned using templates, often with loose control over template creation, leading to template sprawl. Agents must be inserted into every template, and IT needs to enforce agent inclusion in the template-creation process. The difficulty of controlling the templating process leads to VMs not being protected because the agent fails to install.
- Existing VMs that do not have the agent for whatever reason must have the agent installed post creation. This leads to a possibly difficult process of identifying VMs that do not have the agent (and some VMs may be offline) and then installing the agent.
- Offline VMs, assuming they contain the agent, will not be able to update themselves, leading to out-of-date AV signatures or an out-of-date agent. When these VMs come online again, a time window will occur in which they are running with incomplete protection.
- Virtualization and self-service portals have resulted in the easy and quick creation of VMs, leading to an unprecedented scale of logical servers being run. This also creates an increasingly staggering number of software objects (including security agents) that must be managed.

## The Benefits of an Agentless Approach

VMware first introduced the concept of hypervisor-based agentless security with the VMSafe APIs shipped with vSphere 4, in 2009. The VMSafe APIs continue to be supported in the latest vSphere 5 release, although the VMSafe APIs have now deprecated in favour of the newer vShield APIs. The vShield APIs come in three varieties, EndPoint, Edge, and App, which expose different security functionalities. This paper focuses on the vShield Endpoint product and API.

The basic concept of vShield Endpoint is to move malware scanning out of agents that run in every VM and consolidate it into a single VM that runs alongside the other VMs on the host. This security

VM is deployed as a virtual appliance and, through the vShield APIs of the hypervisor, is able to inspect the other VMs running on the server, such as the files and memory.

Moving to this agentless hypervisor-based approach solves the following problems with security in virtual environments:

- **VMs running on the host are always protected.** Agents do not have to be integrated into the VM or template-creation process or installed afterwards.
- **Resources are used more efficiently.** The malware scanner is only instantiated once per server and is able to protect all the VMs on the server, instead of duplicating agents multiple times on every VM.
- **Offline VMs are always fully protected when they come online.** The security virtual appliance is always online and up to date, and this protection extends immediately to any VM without waiting for a signature or agent updates.
- **AV storms are eliminated.** All scanning and update activity is consolidated and coordinated into a single instance per virtualization host.

## Considering Kaspersky Security for Virtualization

Kaspersky Security for Virtualization is an agentless anti-malware protection product designed specifically for virtual environments through its integration with vShield Endpoint.

Key features include:

- Integrates with VMware vShield Endpoint for consolidated agentless protection of all VMs on a vSphere or View host, protecting both server and desktop VMs.
- Utilizes the Kaspersky AV engine and frequent, accurate signature updates for effective detection. The Kaspersky engine is also known for having a small footprint, which requires minimal resources. A remediation process is able to block and remove malware and notify administrators.
- Performs manual, or on-demand, scanning of the VMs, but administrators are also able to schedule scans. Caching prevents the rescanning of files that have already been checked, leading to more efficient scans.

Kaspersky Security for Virtualization also contains the following enterprise deployment, management, and VMware integration features:

- Delivered as a virtual appliance for easy deployment without installing an OS or applications.
- Centralized management console using Kaspersky Security Center 9.0 to provide a single view of virtual, physical, and mobile environments and the ability to generate reports.
- Integrates with vCenter to present information using the VMware constructs of clusters and resource pools.
- Security-profile functionality providing the ability to have different security profiles for different groups of VMs; policies follow the VM even in the event of a vMotion.

### *Challenges for Security in Virtual Environments*

While virtualization is prevalent, uncertainty still exists among customers when it comes to adapting security to virtual environments. Technologies like vShield Endpoint are new, and many customers are unaware that a new approach is available or what the shortcomings are of their imported legacy security solutions.

The vShield APIs are also still maturing. Kaspersky, and any vShield partner for that matter, is limited to what the VMware APIs provide. Kaspersky has many other security technologies such as anti-key logging and Web protection that cannot be integrated due to the current limitations of the vShield APIs. VMware works with its security partners to evolve the API over time to provide greater functionality.

vShield Endpoint is also currently limited to Windows VMs at this time; other operating systems will need to use an agent-based approach.

## Conclusion

Security is an area that is often unaddressed when virtualizing today. However, market trends clearly show that virtualization is a catalyst for change in every part of the datacenter, even the desktop, and security is no exception.

The new vShield hypervisor-based APIs that enable agentless malware protection through products like Kaspersky Security for Virtualization solve many of increasingly visible issues when trying to use traditional, agent-based, solutions in virtual environments. As virtualization deployments expand in scale and complexity and become part of larger private and public cloud and desktop virtualization initiatives, security architectures will have to be rethought and implemented in new ways to keep up with an increasingly virtual and dynamic datacenter.

The ability to manage all protected endpoints (physical, virtual, and mobile) from a single-pane view is also important. Kaspersky Security Center 9.0 provides this visibility and positions Kaspersky well in the marketplace today.

---