

Endpoint Virtualization Explained:

Methods, Benefits, Challenges, and Recommendations for Desktop Virtualization and Application Virtualization

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for Symantec

April 2009

Table of Contents

Executive Summary	1
Introduction	1
IT & Business Benefits of Endpoint Virtualization.....	1
Choosing an Endpoint Virtualization Technology.....	2
Desktop Virtualization	2
Application Virtualization	3
Recommendations for Managing Endpoint Virtualization.....	4
The EMA Perspective	6
About Symantec	6

Executive Summary

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) research shows that virtualization is growing at over 20% annually, and producing measurable cost savings for over 70% of enterprises, as well as many other benefits.

Desktop and application virtualization (or 'endpoint virtualization') are a broad set of mature virtualization technologies deployed to millions of users worldwide.

Desktop and application virtualization (or 'endpoint virtualization') are a broad set of mature virtualization technologies deployed to millions of users worldwide. Various implementations provide benefits including cost reduction, administrative efficiency, easy migration, tighter security and compliance, higher availability, improved productivity, workforce flexibility and mobility, and more.

EMA recommends endpoint virtualization be approached strategically and incrementally, selectively adding multiple endpoint virtualization technologies to existing physical environments, to solve specific business requirements, while always working with

broad, long-term goals in mind. This strategic approach includes a heterogeneous approach to management, integrating management of multiple physical and virtual technologies, and across multiple IT management groups.

Symantec is helping to achieve these goals, with a broad, strategic set of interoperable solutions, which EMA believes puts them in the leading class for endpoint management.

Introduction

ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) research shows that virtualization is growing at over 20% annually. Over 70% of enterprises with virtualization deployments report achieving real, measurable cost savings from hardware and software consolidation, resource efficiency, improved availability, higher productivity, reduced administration, improved security, risk reduction, and improved agility.

The mainstream focus on server virtualization has obscured other technologies like desktop and application virtualization ('endpoint virtualization'), a set of mature technologies that have been available for a decade or more. Today, millions of people – and almost 60% of virtualized enterprises – are using endpoint virtualization from vendors like Symantec, Citrix, and Microsoft.

This EMA white paper discusses the many benefits of endpoint virtualization, how to choose an endpoint virtualization approach, and the new management opportunities and challenges introduced by endpoint virtualization.

IT & Business Benefits of Endpoint Virtualization

Depending on the model used, the benefits of endpoint virtualization include:

- Easier deployment, update, and maintenance – centralized management of virtual desktops and applications, with fewer unique systems and applications, means compatibility testing is faster, administration is easier, and application delivery is faster.

- Faster, cheaper support – end users can get almost instant access to new technologies, access new physical hardware as needed, and get faster delta updates to systems and applications, without any downtime of waiting for a desk-side visit from IT.
- Legacy OS and application support – with virtual desktops and isolation to prevent conflicts, migration to new systems and applications is easier, and users can even access both legacy and updated environments simultaneously on the same physical hardware.
- Better security and compliance – with central control and ownership of applications and data, and fully encrypted desktop environments, environments can be better secured from fraudulent use and accidental exposure, improving both license and legal compliance.
- Balance of control and usability – IT can enforce central policies for specific virtual applications and OS settings, while still allowing users to control their own personal system and application settings, improving user satisfaction while still maintaining IT controls.
- Improved efficiency – both end users and IT waste less time waiting for desktop setup, application delivery, and repairs; software licenses can be quickly and easily harvested and reused; and even lower-powered hardware can run high-powered applications.
- Better availability, DR, BCP – end users benefit from less downtime due to application conflicts, near-instant cutover to new hardware in case of failure, fast roll-back from bad application and OS updates, and virtual access to recovery systems.
- Workforce flexibility – endpoint virtualization provides instant on-boarding for contractors, outsourcers, home workers, and telecommuters, with instant application delivery and update, support for offline and mobile workers, and time-restricted applications to ensure compliance.

Endpoint virtualization is not just one technology. Enterprises should be prepared to deploy multiple solutions together to meet business needs.

Choosing an Endpoint Virtualization Technology

Endpoint virtualization is not just one technology. Enterprises should be prepared to deploy multiple solutions together to meet business needs. When choosing technologies, first look at specific business objectives, user groups, and use cases you need to satisfy – then deploy the approach(es) that will benefit them the most.

Key technologies – including some pros, cons, and typical use cases – are as follows:

Desktop Virtualization

Desktop virtualization is a method of providing an end-user with a complete operating environment (operating system, applications, data, etc.) that is separate from their locally installed desktop operating system. This comes in two main models – remote (server-hosted), and local (client-hosted).

Remote (Server-Hosted) Desktop Virtualization

In this model, the operating environment is hosted on a remote system (normally a data center server), and accessed by the end user across a network. Typical implementations include:

- **Dedicated System** – each user accesses a unique environment, running on a dedicated physical system (often a blade PC). This suits power users (e.g. traders, researchers) who need a personalized environment, dedicated resources, and high availability. However, dedicating server hardware to individual users is expensive compared to other desktop implementations.
- **Shared System (VDI)** – each user accesses a unique environment, running as virtual machines on a shared physical system (often a large server). This suits knowledge workers (e.g. sales, finance) who need a personalized environment, but not dedicated hardware. However, any system slowdown or failure affects multiple users, and VM-based systems require significant hardware resources.
- **Common Desktop** – each user accesses an identical desktop, using Terminal Services on a shared physical system (often a large server). This suits process workers (e.g. CSRs, telesales) who all use a common, low-powered environment. It is an extremely efficient use of server hardware, but allows very limited personalization, and system problems affect all sharing users.

Local (Client-Hosted) Desktop Virtualization

In this model, the operating environment runs locally on the user's physical PC hardware. Typical implementations include:

- **Local OS Virtualization** – additional environment(s) run in a window on top of the standard operating system. This suits users who need independent environments (e.g. Windows and Linux) or multiple application versions (e.g. Office 2003/2007), but it requires detailed technical knowledge, has significant compatibility issues, and requires a powerful desktop PC.
- **Client-Side Hypervisor** – multiple isolated environments run side-by-side on top of the physical desktop hardware (like server virtualization in the data center). This suits primarily IT professionals and power users, and provides hardware independence and mobility. However, it is relatively immature technology, and imposes even greater overhead on the desktop PC.

Application Virtualization

Application virtualization is a method of providing a specific application to an end user that is abstracted from the desktop OS, and not installed in a traditional manner. Typical implementations include:

- **Local Application Virtualization** – the application is installed and/or executed locally within a container that controls how it interacts with other system and application components. This is useful for running multiple application versions, as it avoids component (e.g. DLL) conflicts. However, it can be administratively complex as it obscures some application interactions, and is not 100% compatible with all applications.

- **Application Isolation** – the application is installed and/or executed locally in an isolated ‘sandbox’ that prevents interaction with other system and application components. This suits users that need to run conflicting applications, because it completely isolates applications, but it may also prevent some normal interactions like file access and cross-application communications (e.g. OLE, cut-and-paste).
- **Application Streaming** – the application is delivered across the network, allowing immediate access to core functions, while non-core components are downloaded in the background. This suits users with one-off or temporary application needs, (e.g. contractors), as it allows rapid user-initiated provisioning and easy license harvesting. However, it requires network connectivity for at least the initial delivery/use (streamed applications can be locally cached for subsequent disconnected use), and is not compatible with all applications. Streaming is often combined with Application Virtualization.
- **Web-based Applications** – applications are delivered across the network to a Web browser, with most processing executed on a centralized (Web) server. This supports almost any user, with no installation requirement, on almost any platform, in any location, but it only supports a limited set of applications, requires full-time network connectivity, and has potential security implications.

Ultimately, the endpoint environment is almost certain to be heterogeneous, rather than a ‘one-size-fits-all’ solution, so be prepared to mix and match multiple physical and virtual technologies to accommodate business needs. This incremental approach means virtualization does not have to be a disruptive ‘rip-and-replace’ project.

Adopting an incremental approach means endpoint virtualization does not have to be a disruptive ‘rip-and-replace’ project.

For example, if you have specific ‘high risk’ Web users, you may deploy a standard Web browser as a virtual application on a standard OS, to isolate and instantly remediate Web-based malware. Or if you need rapid on-boarding and scheduled termination for temporary telesales staffs supporting a short-term marketing campaign, you may provide a sales application via application streaming to a remote virtual desktop.

Above all, make sure to look at the big picture and the long-term opportunities, and treat virtualization as a strategy, not just a project. Deploying virtualization in short, tactical bursts is good to establish quick wins and prove ROI, but a short-sighted approach based on hasty departmental decisions can ultimately cause more problems than it solves.

Recommendations for Managing Endpoint Virtualization

As endpoint virtualization changes the way endpoints are deployed – decoupling traditional layers of devices, operating environments, applications, user profiles, and data access – it creates a new opportunity to change the way endpoints are managed. IT should look for management solutions that allow them to provide these layers in flexible, on-demand ways, managing endpoint delivery from a user perspective, not just a technology perspective.

Enterprises should look for management solutions that connect virtualization technologies with physical infrastructure and capabilities.

Enterprises should also look for management solutions that connect virtualization technologies with physical infrastructure and capabilities. EMA research shows that an integrated approach to physical and virtual systems management results in higher uptime, better SLA achievement, lower administration burdens, faster system deployment, faster disaster recovery, and better hardware efficiency.

Management solutions should also accommodate cross-silo human issues to accelerate convergence, improve cross-skilling, and reduce the support load for all management teams. In 67% of enterprises, multiple teams are responsible for managing virtual systems – including network, data center, desktop, and storage. Virtualization needs specialized skills, but these traditional teams must also work together to produce fast, consistent, and error-free outcomes.

Symantec Solutions for Endpoint Virtualization

- **Symantec Workspace Virtualization** – local application virtualization that eliminates application conflicts, reduces testing requirements, provides instant reset for broken applications, and improves administration efficiency, with managed isolation that allows applications to interact in controlled ways with the local desktop and applications
- **Symantec Workspace Streaming** – application streaming that allows instant, user-driven, on-demand application provisioning with offline cache, predictive component download, automatic license recovery, and instant application upgrades
- **Symantec Workspace Corporate** – adds functionality to remote desktop virtualization solutions (e.g. VMware VDI, Citrix XenDesktop, Microsoft Terminal Services) including connection brokerage, single sign-on, roaming printing, and location awareness
- **Symantec Workspace Remote** – Web-based application delivery that provides instant access to corporate virtual applications running under the Symantec Workspace Corporate solution, for full access to any user on any platform, both inside or outside the firewall
- **Symantec Workspace Profiles** – provides additional benefits for remote desktop virtualization, including flexibility to move from system to system, while maintaining a consistent user desktop, yet avoiding otherwise typical log-in delays and profile/data corruption issues
- **Symantec Client Management Suite** – Symantec’s enterprise management solution that provides integrated management and control for delivering, maintaining, and updating both physical and virtual desktops and applications

The EMA Perspective

EMA believes that endpoint virtualization presents mature yet innovative approaches for end user systems and applications, with many remarkable benefits. However, endpoint virtualization does not need to be disruptive, but is best deployed as incremental additions to existing approaches. Enterprises should simply plan to adopt what is needed, when it is needed, where it is needed, combining physical and virtual technologies to solve business-driven use cases.

Symantec is extending the underlying infrastructure into broad, strategic solutions, which puts them in the leading class for endpoint management.

EMA recommends this approach in the belief that there is no single solution for end user computing. Desktops will mix physical and virtual, remote and local. Applications will mix streamed, virtual, isolated, Web-based, and local installations. Ultimately, most end users will actually require a combination of approaches. Regardless of individual technology choices, integrated cross-discipline management of physical and virtual systems is a critical success factor for endpoint virtualization, as is a strategic approach to endpoint delivery.

With connected solutions for application virtualization, desktop virtualization, profile management, and integrated physical and virtual management, Symantec is extending the underlying infrastructure of third party solutions – including leaders like Microsoft, VMware, and Citrix – into a broad, strategic set of interoperable solutions, which EMA believes puts them in the leading class for endpoint management.

About Symantec

Symantec provides security, storage and systems management solutions to help its customers – from consumers and small businesses to the largest global organizations – secure and manage their information-driven world against more risks at more points, more completely and efficiently than any other company. For more information, visit www.symantec.com.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst and consulting firm dedicated to the IT management market. The firm provides IT vendors and enterprise IT professionals with objective insight into the real-world business value of long-established and emerging technologies, ranging from security, storage and IT Service Management (ITSM) to the Configuration Management Database (CMDB), virtualization and service-oriented architecture (SOA). Even with its rapid growth, EMA has never lost sight of the client, and continues to offer personalized support and convenient access to its analysts. For more information on the firm's extensive library of IT management research, free online IT Management Solutions Center and IT consulting offerings, visit www.enterprisemanagement.com.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. "EMA" and "Enterprise Management Associates" are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2009 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com



1862.033009