EXECUTIVE BRIEF

Unified Data Protection for Physical and Virtual Environments

Sponsored by: Symantec

Carla Arend Andrew Buss

April 2014

IN THIS STUDY

This IDC Executive Brief will discuss the evolution and challenges of data protection for virtual environments and how a modern data protection solution can enable both virtualization professionals and storage managers to perform successful backups, but more importantly guaranteed restores. Benefits and challenges of data protection for virtual environments will be discussed, as well as emerging best practices for unified data protection.

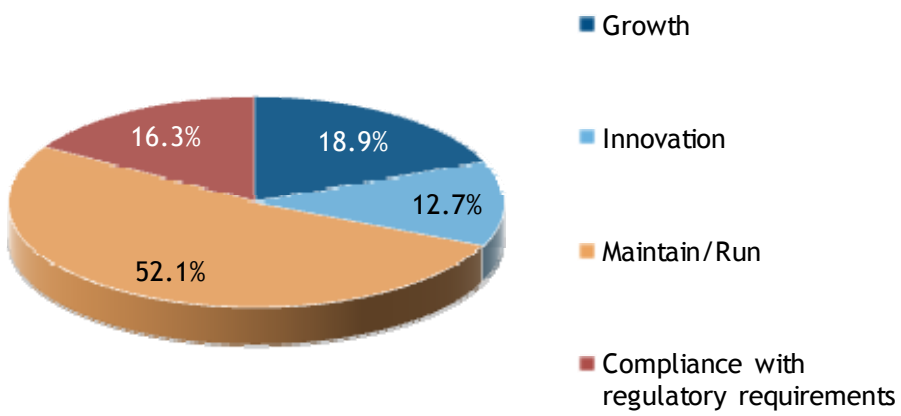
NEW BUSINESS DEMANDS REQUIRE A MORE AGILE IT INFRASTRUCTURE

The nature of business has changed radically over the past few years, with technology playing an increasingly important role in all aspects of the business, from product design and creation, supply chain management and manufacturing through to sales and inventory management, go-to-market partners and customer management. The pace of business is accelerating, and IT is being called upon to support the urgency of the technological changes required.

This need for increasing agility and flexibility has led to a shift in demands on the CIO. With no real increase in budgets, the CIO is responding by changing the way IT is architected and managed to reduce the traditionally high cost impact of routine operations in order to free up budget for investment in growth and innovation.

FIGURE 1

Western Europe IT Budget Allocation



Source: IDC, 2013

Real progress has been made in this area, as highlighted in Figure 1 where operational costs have decreased substantially in real terms in recent years. From as high as three quarters of the overall IT budget a few years ago, improvements in tools and processes have helped to decrease this to around half the total.

A recent IDC CIO survey highlighted several common themes of simplification, innovation, acceleration, and security of the infrastructure as being critical to enabling IT to meet the demands of the business. When the investments required for achieving compliance and scaling for pure growth are factored in, only 12.7% of the IT budget is available to enable innovation.

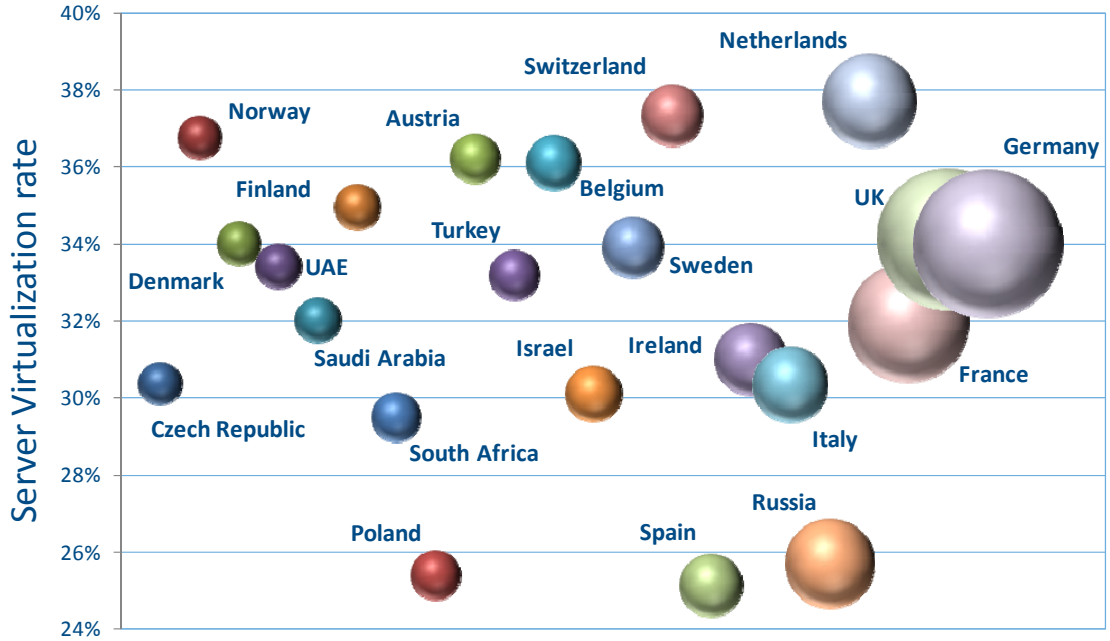
In order to meet these CIO and business objectives and free up more of the budget for innovation, the IT infrastructure needs to become stable and predictable. This means being built more like a commodity utility that is expected to work while being able to adapt as needs change. The key to this is integrating and managing the various parts of the infrastructure – particularly servers, storage and networking – so that they work as a seamless whole, while also freeing applications from being tied to individual physical systems so that they can be deployed where it makes most sense.

VIRTUALIZATION HAS BECOME A BEDROCK OF IT INFRASTRUCTURE

Of the many technologies that IT organizations have deployed in order to become more agile and efficient, virtualization has arguably had the greatest impact. From slow beginnings in the early 2000s, virtualization is now almost universal in uptake in mid- to large-size companies, and increasingly being adopted in the SMB segment. Figure 2 highlights the extent to which companies in the various countries across EMEA now virtualize their new server deployments.

FIGURE 2

EMEA Rate of Virtualization Uptake



Top 22 countries in 2013 FY (Q1-Q3)
Bubble size corresponds to new server systems virtualized

Source: IDC, 2013

Such a rapid uptake of virtualization has enabled many advantages through the efficiency of hardware use and the ability to deploy applications much more quickly. But it has also had a number of side effects which if unchecked can impair the ability to deliver IT services effectively. For example, the delivered performance can be unpredictable when different VMs compete for the same physical resources such as CPU and memory unless service monitoring is implemented effectively. The ease of creation and deployment of virtual machines (VMs) means VM sprawl can quickly take effect, leech compute and memory resources from production systems and eat up storage capacity if the libraries of VMs are not managed effectively.

Another area where virtual environments are running ahead of the IT infrastructure is data protection. Traditionally, the storage team had managed backup and recovery efforts of physical systems. That worked well in the era of dedicated systems and applications, but in the age of virtual machines, distributed applications, and private cloud, the backup system needs to step up and provide information-centric protection in addition to the traditional client-centric approach for physical systems. Because the virtual infrastructure, distributed applications, and private clouds are dynamic and not dependent on a specific physical host or virtual machine, the approach to backup and recovery should encompass new methodologies tailored for such agile environments. It is generally counter-productive to try to manage such environments using the old client-centric way.

In the early days of virtualization adoption, when workloads were largely centered on test and development, this was not such an issue. By 2013, the situation had changed dramatically. While test and development is still the biggest use made of virtualization, it is in the minority of deployment scenarios, as seen in Figure 3. Instead, remote desktop and production applications

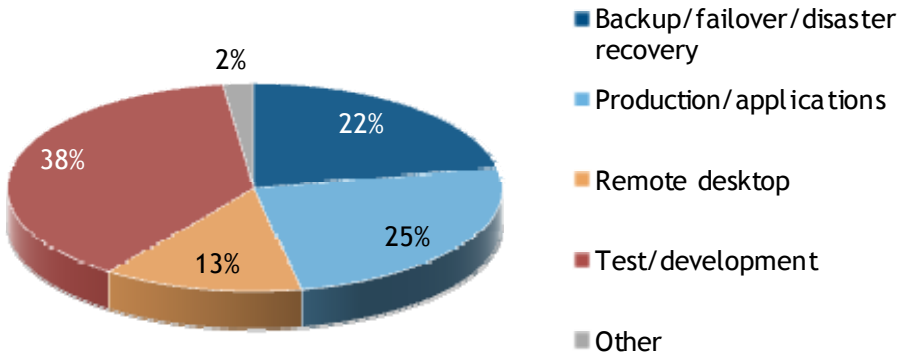
now rival test and development, while significant use is made of virtualization to enhance the reliability, availability, and serviceability (RAS) of the IT infrastructure.

All this dependence on virtualization across the IT infrastructure means that protecting the virtual infrastructure is now as important as protecting the physical always has been.

FIGURE 3

EMEA Virtualization Deployment Scenarios:

Share of Server Virtualization Usage Solutions in EMEA by Virtual Server Unit



Source: IDC End User Survey 2013
n=2,203 companies applying server virtualization

CHALLENGES FOR DATA PROTECTION IN MIXED ENVIRONMENTS

The end result of this march of virtualization has been that the administrators of virtual infrastructure are increasingly responsible for data protection surrounding critical business infrastructure. The rapid pace of technology development has meant that in many cases, the traditional products focused on physical data protection could not offer the flexibility and agility needed to protect the new virtual infrastructure.

Point products that specialized in protecting virtual machines were often purchased specifically to solve this need. These products were developed to cater for the enhancements that virtualization can bring to IT, such as being able to rapidly recover virtual machines directly from a backup to a target host without further processing, or to more efficiently back them up by storing only the changes that exist between a master virtual machine image and clones that have some customizations applied.

What has emerged is two parallel and often fragmented data protection environments, one for the physical infrastructure and one for the virtual infrastructure, with very little commonality or integration.

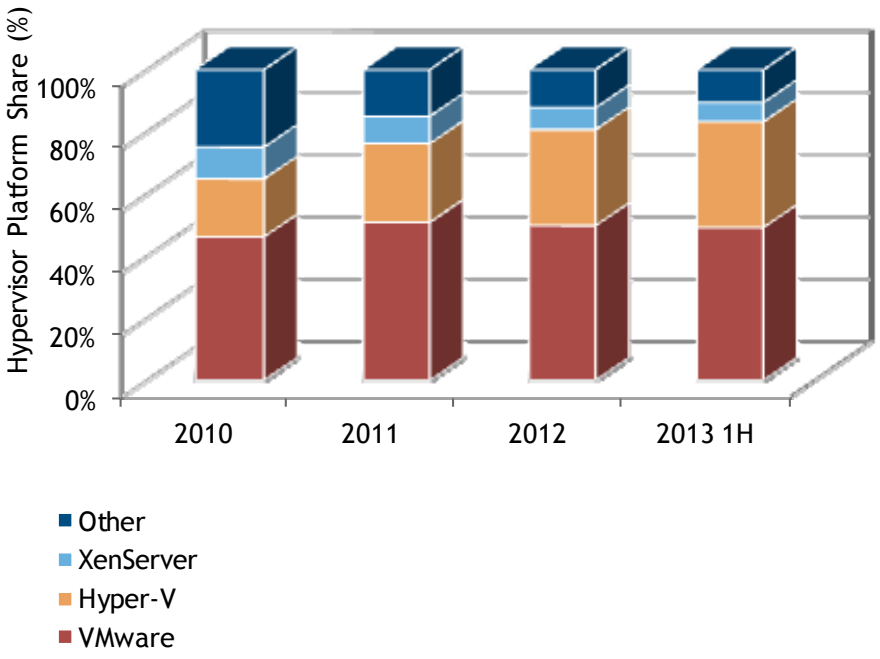
This approach can solve the immediate pain point of ensuring that data protection is adequately catered for in both physical and virtual environments. However, it does create longer-term issues around management and consistency when it comes to business continuity and compliance, as well as increasing costs through operations overheads as well as increasing the risk of errors and failure due to manual intervention across systems.

Another issue that has emerged when it comes to data protection in the virtual infrastructure is the question of hypervisor support. For many years, VMware was the default choice in many installations. More recently, Microsoft has emerged as a contender while XenServer, KVM, and Oracle, among others, are also in active use in many companies, as can been seen in Figure 4.

FIGURE 4

Hypervisor Platform Share in EMEA:

New Hypervisor Deployment by Host Units



Source: IDC, 2013

Many data protection solutions for virtual infrastructure have focused on specific hypervisor vendors, or have had to take a least common denominator approach to supporting features and capabilities which reduces the overall benefits of the solution.

Where a data protection solution focuses only on the virtual environment or on a particular hypervisor vendor, it raises issues of migration and compatibility. Physical to virtual is an important migration and restoration route, but so is virtual to virtual, as well as virtual back to physical. All of these use cases need to be catered for to enable a seamless data protection environment across both physical and virtual infrastructure.

If a lot of integration work and effort are needed to move virtual environments between these areas, it effectively creates islands of infrastructure that are separated from one another and that require dedicated skills and effort to manage. This is antithesis to the long-term goals of simplification, standardization, and agility that the business and CIO are aiming for, and so a new approach is needed.

UNIFIED DATA PROTECTION ACROSS PHYSICAL AND VIRTUAL ENVIRONMENTS

When it comes to data protection, many companies have taken the approach of implementing "best-of-breed" solutions to protect their virtual infrastructure, while leaving their existing solutions in place to continue to protect the physical assets already in use. While convenient and relatively quick and easy to implement, this has led to broader issues surrounding integration, management, and consistency.

What is needed ideally is a single product solution with a broad set of capabilities that is able to implement data protection seamlessly across both physical and virtual environments, and across the different hypervisor technologies from all the leading vendors.

This might seem like the Holy Grail and unachievable in practice, but the reality is that unified data protection suites are starting to become feature rich and very capable. The end result is that these "best-of-need" solutions are able to deliver a significant amount of the capabilities of the "best-of-breed" vendors, but with the benefits of integration and management across the variety of physical and virtual scenarios.

BEST PRACTICES FOR DATA PROTECTION OF VIRTUAL ENVIRONMENTS

With the increasing move towards private cloud and the software defined datacenter, IT operations are focused on removing individual isolated "islands" within the infrastructure that need their own operations, skills, and management. When virtualization started as a niche technology, it required specialized tools for backup and recovery. Now that it has become the preferred method of deployment in most cases, adjacent processes such as backup and recovery need to be managed across the entire infrastructure, both physical and virtual, and cannot be a patchwork of point solutions operated independently.

Data protection and recovery needs to fit seamlessly into the higher level automation and orchestration layers that are being enabled now that virtualization is so well established. Eventually, the data protection function needs to be so mature and embedded that it will become one of many attributes of a service level that is defined for an application.

This can realistically only be achieved through the use of an integrated data protection platform. The use of multiple point products deployed individually makes this difficult to achieve unless significant efforts are made to integrate the various elements.

One way to accelerate the implementation of unified data protection is to consider deploying an appliance that has all the necessary hardware and software in one self-contained unit. This means that the solution can be up and running and fully supported in a very short time with all the necessary software and hardware but without the overhead of having to justify and purchase separate servers, storage, and software licenses.

Workload migration from physical to virtual and back again, as well as between different hypervisor environments, is critical functionality that the data protection solution should provide. By doing so, IT managers can move workloads seamlessly between different environments and also to external third-party compute platforms as desired.

BENEFITS OF UNIFIED DATA PROTECTION FOR THE IT INFRASTRUCTURE

The ability to define a single data protection management policy for different physical and virtual environments greatly simplifies the process of backup and recovery. Consistency makes compliance easier to achieve, as well as making it more effective to demonstrate continuing compliance. Additionally, the integrated approach avoids fragmentation through incompatible islands of data protection, promoting operational efficiency and reducing ongoing operational expenses, which is a key target for CIOs looking to invest in growth opportunities.

Support for the multitude of mainstream hypervisor implementations enables VMs and workloads to be spun up and run on the platform that makes most sense according to the SLA. The license and support costs of the different hypervisors vary greatly. The freedom to choose the appropriate platform — whether for factors such as ISV support, performance, cost reduction or manageability — can help to optimize the ongoing costs of running workloads by enabling them to run where they are most suited rather than being constrained to a single hypervisor environment.

The data protection library can act as another layer of storage. The virtual machines being stored in the library can be spun up directly without needing to be restored to an intermediate storage medium. This means that files and data can be recovered quickly from the virtual machines by spinning them up, while whole applications and services can be recovered back to full operational status directly from the backup to the target host, ensuring minimal service interruptions.

This ability of the data protection solution to act as another layer of storage also means that if the solution vendor also has broader storage management capabilities, these can make use of the data protection storage to optimize the use of the entire storage stack and free up valuable space for volatile data on high performance storage while ensuring that common storage technologies such as dedupe, compression, encryption, and replication can also be made available to optimize the data protection capabilities.

ESSENTIAL GUIDANCE

Virtualization is now an essential technology to deliver the next generation of automated IT service delivery through private and hybrid/public cloud, and most organizations will be making increasing use of it in the coming years as they evolve the IT infrastructure towards a software-defined data center (SDDC).

Choosing a vendor with a comprehensive portfolio of data protection tools that work across physical and virtual environments, including all the mainstream hypervisor implementations, will be essential to deliver end-to-end services with agility and quality, while ensuring that no individual islands of services are left to be managed separately.

It will be an additional advantage if a vendor's data protection capabilities are also complemented by a broader portfolio of storage management capabilities that can make use of the data protection capabilities to help optimize the storage and management of virtual infrastructure images and data.

IDC advises that any data protection solution should protect both the physical and virtual infrastructure, as well as supporting the use of any of the top 5 mainstream hypervisor solutions in common use.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1000 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For more than 48 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

Chiswick Tower
389 Chiswick High Road
London W4 4AE, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2014 IDC. Reproduction is forbidden unless authorized. All rights reserved.