

WHITE PAPER

Best Practices for Windows Vista Planning, Migration, and Ongoing Management

Sponsored by: Symantec Corporation

Frederick W. Broussard

June 2007

IN THIS WHITE PAPER

This IDC White Paper examines best practices for migrating to Windows Vista, including premigration planning, performing Windows Vista migrations, and supporting ongoing post-migration activities such as PC system and data security, protection, and management. The White Paper also discusses Symantec's life-cycle management solution approach for rapid, reliable, and secure Windows Vista migration and ongoing management.

IDC OPINION

Performing operating environment migrations, such as Windows Vista migrations, has become easier because of capabilities contained within the operating systems (OS) themselves, such as the Windows Easy Transfer migration tool that comes with Vista. However, this does not mean that the operating environment provides a complete or integrated solution for migration or that tools used previously to create and maintain images, perform deployment, migrate users' personality settings, or securely retire systems are now obsolete.

Migration to Windows Vista requires significant premigration planning. The initial planning should incorporate inventory discovery and assessment for the current environment. This information allows identification of PCs that fall short of the minimum system requirements and creation of a plan for upgrading or securely retiring these systems. Determination of whether migration will be carried out to new or existing hardware identifies whether users' personality settings need to be captured.

During the design phase, organizations should use security tools to ensure an uncompromised migration footprint and should consider the applications and settings required in the base image, creation and testing of a base image suitable for individual corporate needs, performing system and data backups as an insurance policy prior to migration, and capturing users' personality settings if required.

The actual migration involves deployment of the new image and restoration of users' personality setting packages. Post-migration activities for ongoing system management include providing regular patching, system, and application updates; maintaining a secure and consistent PC environment; ensuring user data is backed up and restorable; and securely retiring systems. Automation of routine IT tasks will free up administrators to perform other high-value projects and tasks.

Because IT organizations have had to deal with migrating from Windows 2000 to Windows XP, as well as from Windows NT to Windows 2000, vendors have had plenty of experience in creating and developing solutions providing automated capabilities for handling the end-to-end process of migrating an organization from one operating environment to another. Further, as vendors have moved toward process-based management solutions required by management frameworks such as ITIL, solutions are available that take a life cycle-based approach to not only the migration but also the subsequent ongoing system management. IT departments that need to perform rapid and reliable OS migrations and ongoing management of systems and ensure continuous data and systems protection should consider whether Symantec's Vista migration and ongoing management solutions are appropriate for their organizations.

SITUATION OVERVIEW

Introduction

Life-cycle management requires that IT departments periodically refresh software applications residing on the PC, as well as the PC itself. IDC's view of the overall process is described in Figure 1, which shows that IT organizations start by planning new hardware or software installations within their organizations. Following discovery and assessment of hardware and software inventory, an overall plan is defined. They then create a base image, capture user personalities, and perform any necessary integration testing and development. Deployment of the image is then followed by restoration of user personalities if applicable. Once the base solution is implemented, focus is then placed on keeping the OS, software, and configurations secure, updated, and maintained and upgrading or migrating to new versions over time as appropriate. Systems are retired eventually, and the cycle is started again.

FIGURE 1

Life-Cycle Management

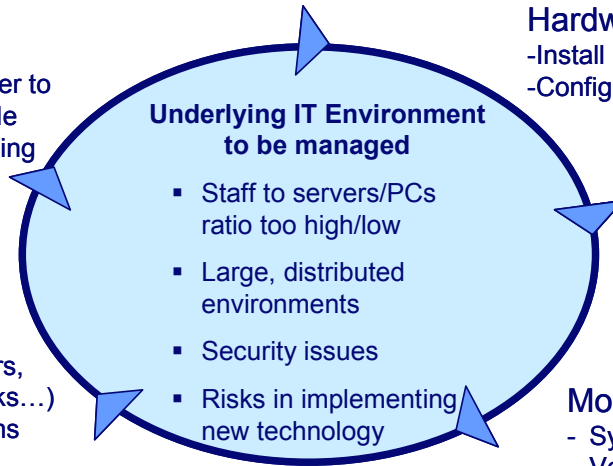
Using manual and automated processes to....

Plan Projects

- Assess existing inventory
- Determine whether to upgrade or recycle
- Scheduling/planning rollouts

Deploy Software and Hardware

- Install new applications
- Configure servers/PCs/PDAs



Retire Systems

- Hardware (servers, PCs, PDAs, kiosks...)
- Operating systems
- Applications

Monitor and Repair

- System stability
- Version compliance
- Patch installations

Migrate/Upgrade

- App v2.x to v3.x
- Win2K/WinXP to WinVista
- Data files

Source: IDC, 2007

Broader Organizational Considerations

Because life-cycle management requires a systematic approach to managing changes to and configurations of desktops and laptops, IT departments must also consider overall corporate requirements such as:

- ☒ **Minimizing project costs and risks.** A basic requirement of any solution is to keep costs to a minimum and allow testing to identify and mitigate or eliminate potential risks.
- ☒ **Minimizing end-user disruption/impact.** End-user downtime and loss of productivity have a significant impact on all organizations. Minimizing the impact of activities on end users is an important consideration for all IT staff, from the CIO on down.
- ☒ **Minimizing IT resource and time overheads.** For planning and performing OS upgrade/migration projects as well as ongoing management of systems within the IT environment, IT administrators should consider solutions that can automate routine IT tasks, streamline processes, and allow tasks to be performed remotely.

- ☒ **Planning appropriately to ensure successful migration.** It may take IT departments 12 to 18 months to successfully plan for a Windows Vista migration. IT administrators also need to consider remote and mobile workers who may have infrequent network access and their many devices.
- ☒ **Ensuring overall security of the environment and complete data and system availability before, during, and after migration.** Data protection is critical in order to ensure that users can access their data and are kept productive at all stages of the migration.
- ☒ **Supporting mixed Windows environments (e.g., Windows XP, Windows 2000, Windows Vista).** Many organizations will replace systems over time as older systems are retired rather than perform a mass migration. Life-cycle management solutions need to be capable of successfully managing mixed Windows environments.

Migration Paths to Vista

Windows Vista rolled out to retail channels on January 30, 2007, but customers buying volume licenses were able to purchase Vista in November 2006. Obviously, decisions on whether and when to migrate started much sooner. Client-based operating environment migration paths include the following.

- ☒ Windows 2000 to Windows Vista
- ☒ Windows XP to Windows Vista
- ☒ Windows 2000 and Windows XP to Windows Vista
- ☒ Bare metal to Windows Vista
- ☒ Selection of Windows Vista edition

Evaluation should be undertaken to determine sufficient Windows Vista capabilities to meet individual organizational requirements and ensure optimum performance today and in the foreseeable future. Part of the evaluation is to select the appropriate Windows Vista edition and to specify the hardware configuration requirements needed to support it. While Windows Vista offers an enhanced user experience, the range of Windows Vista functions that can be supported is governed by specific hardware requirements. Windows Vista Capable hardware can support core Windows Vista functions. Current guidance suggests that PCs with at least 512MB of RAM, at least 800MHz processor, and DirectX 9 Capable GPU are Windows Vista Capable.

Windows Vista Premium Ready hardware provides support for enhanced Vista features such as 3D Aero glass, enhanced visual quality, and glitch-free window redrawing. Windows Vista Premium Ready configurations include PCs with at least 1GB of RAM, 1GHz 32-bit processor, 40GB hard drive with 15GB of free space, and Windows Aero Capable GPU. Much of the laptop and desktop installed base currently within an IT organization may include machines configured with only 128MB or 256MB of RAM, far less than the 1GB recommended for the optimum user experience. As such, a crucial step in migrating to Windows Vista will be verifying whether existing hardware and software are compatible with the new operating environment and will offer the required level of performance for individual organizational needs.

Vista Desktop Migrations: Before, During, and After

Corporate IT departments realize that they must look for tested solutions that automate the migration process from beginning to end and ensure that systems remain available, secure, and well-managed throughout the entire process. The first phase starts with creating an effective and comprehensive migration plan prior to the actual migration. Many organizations may require 12 to 18 months of planning to ensure they can successfully migrate to Windows Vista. We cover each of the migration phases in detail within this section. Some general considerations across the entire end-to-end migration process include the following:

- ☒ The IT environment must be continuously protected from viruses, trojans, worms, and other malware, typically by antivirus or other endpoint security software.
- ☒ Individual user data that is stored on the PC must be protected against accidental deletion, which may occur as the result of IT department actions during migration or migration planning and testing.

Before: Planning and Designing the Vista Migration

During the initial Vista migration planning stage, organizations require software solutions that can help with the discovery and assessment of the current environment as well as determination of software and hardware compatibility for the new operating environment. Organizations also require software solutions that can assist with the design and creation of images and the capture of user personality settings from existing machines. User personality migration is crucial to ensure that an existing user's data, unique application settings, and Windows configuration settings are maintained and preserved during the migration. A user personality includes a user's personal data files, such as Microsoft Word and Excel documents, and settings such as wallpaper, desktop shortcuts, Internet bookmarks, networked printers, mapped drives, and regional and power settings.

Key steps involved in the premigration phase include the following:

- ☒ Discovery of hardware and software assets in the current environment
- ☒ Assessment of system hardware configurations — Vista Capable or Vista Premium Ready
- ☒ Assessment of system software compliance
- ☒ Determination of licensing implications
- ☒ Upgrade or retirement of systems that fail to meet minimum requirements
- ☒ Identification of group of machines to receive the new operating environment
- ☒ Documentation of overall migration plan — network infrastructure and details, deployment methodology and schedule, forecast bandwidth requirements

- ☒ Capture and storage of PC user personalities (user data, application settings, and Windows configuration settings)
- ☒ Design and creation of a base Vista image
- ☒ Scan of premigration environment for security threats
- ☒ Backup of systems and data as a premigration insurance policy

With the proliferation of software solutions available and the use of in-house-developed solutions, IT organizations have plenty of choices when thinking about migrating software from one desktop or laptop to another. And with the introduction of process management frameworks such as ITIL that implement changes on a best-practices basis, it's easier to think about these types of life-cycle changes within a systematic process in order to minimize unintended changes.

Premigration Planning Best Practices

IT organizations are best served by taking an automated, process-based approach to determine the number of PCs in the IT environment, determine the hardware and software inventory of those PCs, identify PCs that need to be upgraded or retired, and identify and group PCs that meet the minimum hardware requirements. From there, IT managers can determine the potential costs associated with moving PCs to the new operating environment and budget appropriately for the project. IT organizations should use software-based solutions that do not require each PC to be visited because the more PCs under management, the larger and more time consuming this task is. Software solutions with remote management capabilities will decrease or eliminate the need for an administrator to travel to update PC configurations. IT organizations should consider software solutions that assist in automating and performing the following tasks:

Hardware and Software Discovery and Assessment

- ☒ **Remote capabilities.** IDC recommends that organizations — rather than physically visit hundreds or thousands of machines individually — implement a solution that automatically and remotely discovers and inventories the RAM, hard drive, video card, and processor capabilities of all PCs on the network.
- ☒ **Single centralized console.** IDC suggests that organizations use a single console that consolidates into one view the number of PCs and the PCs' hardware and software configuration. Armed with this data, organizations can then determine the costs associated with physically upgrading PCs and the associated labor costs in testing applications on the new environment, license management requirements, migration and data backup requirements, security requirements, and post-migration management needs.
- ☒ **Built-in inventory filters.** Built-in inventory filters based on the minimum specifications for Vista Capable and Vista Premium Ready systems can save significant time and effort in identifying machines that are Vista ready. Organizations that have specific requirements beyond the minimum Vista specifications should ensure that any prebuilt filters can be easily modified.

- ☒ **Secure retirement of systems.** Systems that do not meet the minimum migration requirements and are no longer required need to be securely retired. Formatting or deleting data simply removes file references, but not the file contents, from the hard disk. Files are still recoverable by software means. The only sure way to securely delete data from the drive is to use a tool that completely overwrites the hard drive and deletes the data. IDC recommends use of a software solution that supports the industry's highest "disk wipe" standards to minimize security exposure and unnecessary organizational risk: the U.S. Department of Defense NISPOM (National Industrial Security Program Operating Manual) DoD 5220.22-M (1995) and the Assistant Secretary of Defense Memorandum of Disposition of Unclassified DoD Computer Hard Drives (2001).

- ☒ **Scan of premigration environment for threats.** Prior to the actual migration, organizations should fully scan the environment, typically with endpoint security software, to ensure undiscovered threats such as viruses, trojans, worms, and other malware are not transferred to the new OS, thus compromising the new OS and infrastructure upon boot-up.

Capture and Storage of PC User Personalities (User Data and Settings)

- ☒ **User migration templates.** IDC suggests usage of software solutions that offer templates that can be defined for different departments or groups to minimize the amount of work required to migrate multiple users. In addition, wizard-driven capture and restore of packages can help to simplify and speed user migration. Organizations that use PC user personality migration can significantly reduce post-migration support time and costs as well as minimize the risk of end-user downtime or lost productivity.

- ☒ **Broad user migration application support.** When migrating user data and settings, organizations must ensure that their chosen software solution supports a broad range of applications. The vast majority of available solutions offer support for Microsoft's applications; however, organizations should also consider other core applications in use, such as Cisco VPN, Lotus Notes, and Adobe Acrobat Reader.

- ☒ **User migration policies.** Policies that restrict users from adding unauthorized files such as MP3s to the migration package, or that prevent users from modifying migration tasks, can assist in ensuring a well-managed and secure environment.

- ☒ **User migration package local storage.** Storage and preservation of PC user personality packages and files in a client staging area on the local machine during a migration or deployment allow images and other resources to be distributed in advance of a task. Local storage also helps to minimize network traffic because files do not need to be sent back and forth from a server or a second machine. All of the files in the client staging area are immediately available after migration or deployment, thereby minimizing any downtime.

Creation of Base Vista Image

- ☒ **Hardware-independent images.** Best practices require that duplication should be eliminated wherever possible. Minimizing the overall number of unique machine configurations will simplify both image creation in the immediate term and image management on an ongoing basis. IDC recommends software that supports creation of a single Vista image suitable for deployment to multiple machine types (hardware-independent images) using Windows Sysprep.
- ☒ **Easy image editing.** IT administrators benefit from images that can be easily edited to simplify ongoing management in the future.
- ☒ **Comprehensive base image configuration.** IDC suggests that PC configurations include antispyware, antivirus, and other system security and management solutions as part of the base image to minimize exposure to risk following deployment and get end users up and running as quickly as possible.

Application Testing

One of the biggest obstacles in Vista migration is the application testing necessary to determine the effects of the Vista OS on existing applications. Many third-party commercial applications have been tested with Windows Vista, but IT managers face the challenge of testing customizations to those third-party applications, as well as testing applications written in-house for company use. A successful migration process must incorporate and allow for testing within a lab environment.

Support for Mixed OS Environments

Many organizations will need to manage mixed Windows environments in the short or long term. Such organizations should keep an eye on moving toward managing a single environment, and they should select software solutions that support mixed configurations for the migration process and incorporation into the base image.

Phased Rollout

The IT department must determine which organizations will receive the new operating environment and when. A phased rollout also helps in determining which groups may experience problems with the resulting operating environment and when those problems should manifest themselves. And of course, rollback capabilities should be considered in case something goes wrong during deployment so that the new OS, applications, and patches can be removed and the PC returned to its original state.

Data Security and Protection

Because of the destructive nature of OS migration, IDC recommends that in addition to capturing PC user personality packages, organizations should back up individual end-user data to another location. Where multiple machines are being migrated that require data backup, a centralized location must exist that is capable of handling this volume of backup data. Furthermore, Windows Vista supports security-enhancing features such as user account control, network access control, and authentication, but it does not provide other baseline security capabilities. Planning should take into account how antivirus and other security measures will be deployed with the new operating environment.

During: OS and User Migration

When performing the actual migration, organizations require software solutions that can assist with rapid and reliable deployments and restoration of user packages. The key steps necessary to migrate users to the new operating environment include the following:

- ☒ Targeting machines to receive the new operating environment
- ☒ Deploying base Vista images
- ☒ Restoring any previously captured PC user personalities (user data and settings) onto the new machine
- ☒ Scanning the new environment for security threats to confirm the uninfected security state of the system

Migration Best Practices

Effective premigration planning allows IT organizations to anticipate where problems will surface and how to address them. The actual migration phase really comes down to executing on plans and fixing problems as they occur. This means IT organizations should already have put into place the following practices:

- ☒ **Targeting of Vista-ready machines.** Prebuilt inventory filters based on the minimum specifications for Vista Capable and Vista Premium Ready systems can save significant time and effort in creating a dynamic group of machines that are Vista ready. When organizations are targeting machines for deployment, IT needs to ensure that the machines as well as the people within the group haven't changed from month to month.
- ☒ **Rapid and reliable image distribution.** Vista images must be distributed in a way that doesn't cause undue bandwidth constraints on the network but that allows for rapid and reliable automated distribution to the many PCs within the environment. IT organizations can lower costs by distributing the new operating environment using either a unicast or a multicast deployment approach. With a unicast approach, the images are deployed to one machine at a time in turn. With a multicast approach, PCs are designated as peers and then are able to act as distribution points for pushing out the image to multiple machines simultaneously. The multicast approach speeds delivery of the image to all machines and significantly minimizes network traffic because the image travels over the network only once.
- ☒ **End-user migration notification and support processes.** A notification process should be in place to alert end users that the migration is taking place and to advise end users of what to do if they experience any unusual issues following the migration. End users should be advised as to what a problem related to the migration might look like and to alert the service desk of any problems. Upon notification of an issue during the deployment or overall migration process, the IT department should be able to fall back to a previous state for PC configurations. When a PC fails to receive the new operating environment for whatever reason, the solution must allow identification of the PC so that another attempt can be made.
- ☒ **Project schedule.** An overall project schedule should exist that tracks that the migration activities are happening and that rollout of the new operating environment is occurring as planned.

After: Ongoing Management of Systems

For ongoing management of systems, organizations require software solutions that can perform ongoing maintenance such as secure system retirement and updates of desktop software and configurations. Post-migration activities center on data restoration and availability and PC security. Data availability is handled by using processes that back up and restore data to the PC. PC security is handled by similar processes aimed at ensuring that the antivirus and antispyware solutions are in place, and up-to-date, as soon as the PC is back on the network and in the user's hands. PC security requires:

- ☒ **Recovering individual end-user files.** Individual end users accidentally delete files, suffer file corruption, have their laptops stolen, drop their laptops, and receive and inadvertently open virus- or worm-infected emails, among other disasters. More attention is typically paid to the data stored on servers than to the data on individual PCs.
- ☒ **Migrating or upgrading new systems.** Moving from one operating system or software application to another is a straightforward process for one machine, if machine hardware types are similar. It is a larger challenge for an organization moving dozens, hundreds, or tens of thousands of desktops and/or laptop machines. Each PC hardware configuration must be tested with each new software configuration on which the operating system resides; thus, as two types of laptops are tested against four combinations of software configurations, an organization would have to test eight combinations of software and hardware.
- ☒ **Addressing PC protection from the very beginning with the latest in antivirus and antispyware.** This is necessary not just to protect the machine itself but also to ensure that the overall IT environment is protected from a threat introduced through an infected machine being allowed access to the network. While Microsoft has increased security through features such as User Access Control, Authentication, Network Access Protection, and Microsoft Forefront Client Security, third-party solutions may still be deployed to ensure clean migration and ongoing operations.

Post-migration and Ongoing Management Best Practices

IDC research has shown that IT organizations that don't have consistent sets of tools, desktop configurations, and policies aimed at consistent administration of these configurations and tools should move toward post-migration best practices that center on standardized PC management. This means:

- ☒ Having an overall three- to four-year strategy for the desktop, and as part of this strategy, deploying a standardized desktop that minimizes the number of different hardware and software configurations.
- ☒ Managing these minimized hardware and software configurations from a central console. Additionally, the standardized configuration deployed should minimize an end user's ability to change that configuration, thereby maintaining overall PC security, reliability, and application compatibility.

- ☒ Proactively addressing PC security with antivirus, antispysware, and patching. An integrated configuration that provides these functions embedded in a single solution helps standardize management across all PCs.
- ☒ Having PC disposal policies and tools for securely wiping data from PCs that are being retired. IT administrators should be aware that when files are deleted from a disk on a PC through the operating system, the operating system doesn't erase the content of these files from the disk. It deletes only references to these files on the hard drive. Contents of the deleted files continue to be stored on the disk and can be easily restored using data recovery utilities. Most enterprises lack adequate PC disposal policies and give away critical data when they discard old PCs, especially when proper file deletion procedures aren't followed. Most government agencies now stipulate that hard drives must be thoroughly cleansed before they are disposed. Disk reformatting as an alternative to cleansing corporate data from PC hard drives is a lengthy and laborious process and not always completely secure. Moreover, reformatting doesn't inhibit the ability of a low-level tool recover the data. IDC recommends use of a software solution that supports the industry's highest "disk wipe" standards to minimize security exposure and unnecessary organizational risk.

Over time, as IT organizations adopt the technology necessary to implement and work with a standardized PC configuration, they can then move forward to increasing their ability to:

- ☒ Evaluate new technologies
- ☒ Improve IT governance and ensure the IT department is delivering the required level of service to end users and business organizations
- ☒ Invest in virtualization technologies that benefit the organization through enhancing system flexibility in meeting the needs of the overall business
- ☒ Speed delivery of applications to end users through the entire acquisition and test process, thereby increasing end-user capabilities that much faster

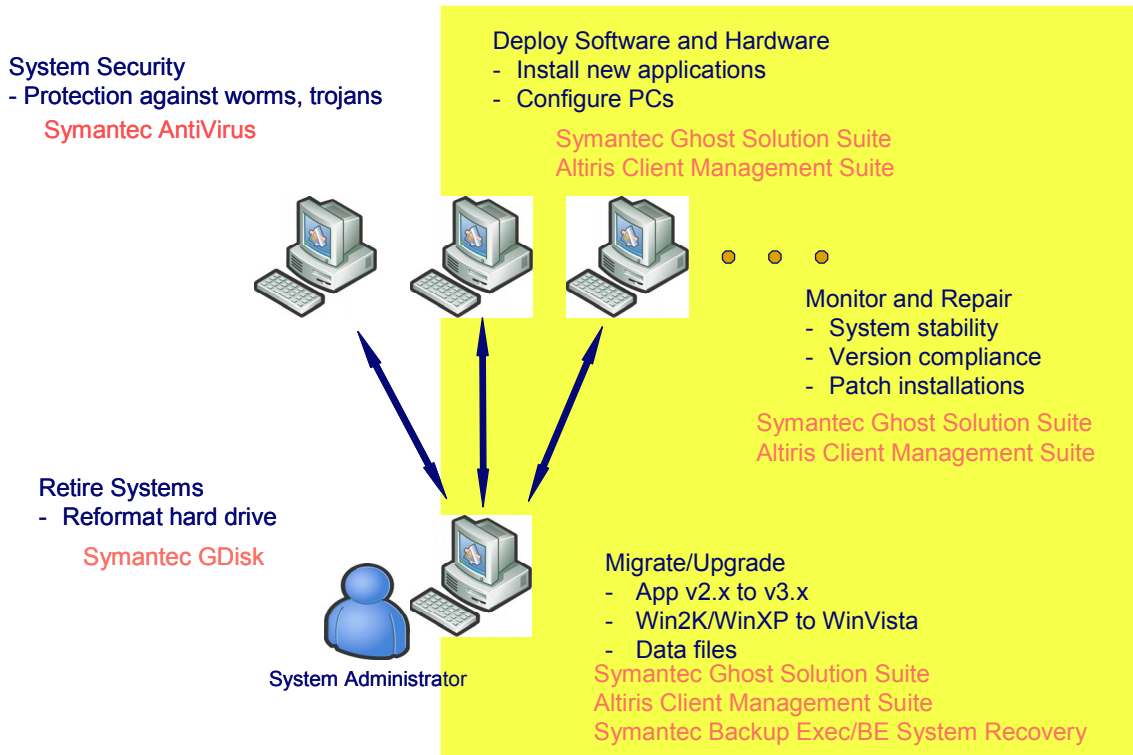
Symantec's Overall Management Solution

Symantec has several solutions that work together to manage Windows systems throughout their life cycles. Symantec provides solutions for premigration planning, migration, and post-migration ongoing management of Windows systems, a backup and recovery solution to store end-user data and protect complete Windows Vista systems, and a security solution to protect machines from infection before migration and after migration is complete.

Figure 2 shows specific areas where solutions support PC life-cycle management from PC acquisition to secure system retirement. Symantec's management solutions assist in project planning, design, deployment and migration, and ongoing systems management to ensure stability and patch installations; performing migrations; and securely retiring systems. These solutions are presented in more detail below.

FIGURE 2

Symantec Solutions Usage in the Life Cycle



Source: IDC, 2007

Premigration Planning

Symantec's product portfolio helps IT organizations manage a number of premigration tasks and gives IT organizations flexibility in executing those tasks. Specifically, the portfolio covers:

- ☒ **Hardware and software discovery and inventory.** Symantec provides solutions that IT administrators can use to discover hardware and software inventory and quickly and easily identify systems requiring upgrade or retirement. Built-in filters based on the minimum Windows Vista specifications enable fast and easy identification and targeting of Vista Premium Ready and Vista Capable PCs.
- ☒ **Collection and migration of PC user personalities (user data and settings).** Symantec offers integrated user migration, enabling all migration tasks to be performed from a single central console. Templates simplify migration of multiple users. Symantec provides support for a broad range of popular applications for user migration well beyond just Symantec and Microsoft applications.

- ☒ **Creation of a customized corporate Vista image to suit individual organizational needs in terms of software applications, etc.** Symantec's solution can be used together with Windows Sysprep to create a hardware-independent Vista image suitable for deployment to multiple machine types. This means that it includes the capability to create an image with the feature that automatically searches for the appropriate drivers based on the registry keys within the image and to provide those keys to the underlying hardware. This capability allows an image to be created on one hardware platform, yet be transported to another platform, regardless of RAM, number or type of CPU, hard drive size (as long as the new image is not smaller than the original image), or even manufacturer. Symantec offers the choice of using either file- or sector-based imaging.
- ☒ **Simplified migration and management.** Symantec's solutions contain preconfigured tools to identify PCs in various configurations and wizards to help design and execute the migration.
- ☒ **PC configurations.** Security event logging in the console enables critical system and regulatory compliance.
- ☒ **Automated data security and protection.** IT administrators can embed the Symantec security solutions into the base image for the PC and use this as the starting point for ongoing management with Symantec's security and data protection solutions after the migration.

During Migration

Effective planning allows IT organizations to anticipate where problems will surface and determine how to address them. The actual migration phase really comes down to executing on plans and fixing problems as they occur. This means IT organizations should have already put into place the following:

- ☒ Symantec's multicast deployment approach for migration allows for rapid and reliable image distribution through a multicast approach. Images, software applications, or individual files can be distributed to multiple machines on the network simultaneously. Symantec's solutions also include network bandwidth management to ensure that updates do not overwhelm the network and to reduce overall network traffic when compared with a one-to-one unicast deployment approach.
- ☒ Procedures and policies alert users that the migration is taking place and that they should notify the service desk of any problems.
- ☒ Symantec's data and system backup capability ensures a safe fallback position in the event that there are issues with the Vista rollout.

Post-migration and Ongoing Management

Symantec's solutions for migration enable the post-migration environment to be effectively managed through to retirement as follows:

- ☒ Ongoing regular inventory scans can mean that the PC configuration can be compared with the post-migration PC configuration for changes. PCs can be scanned for security threats to confirm the uninfected state of the system. The solution can then be used to push out applications, patches, and updates as necessary.
- ☒ All of the Symantec solution capabilities for identifying and managing user state and configuration settings as well as security settings; distributing and managing antivirus and antispyware solutions; patching and updating PCs; and managing multiple Windows desktop operating systems and day-to-day data and system protection during the migration can be used after the migration. These solutions can collectively help lower overall system life-cycle costs by automating manual actions to manage the PC configuration and ensure complete data and systems protection.
- ☒ Symantec solutions can completely wipe corporate data from a PC hard drive to provide secure data disposal and PC retirement. Symantec says its solutions meet the industry's highest disk wipe standards consistent with the U.S. Department of Defense Standard DoD 5220.22-M.

FUTURE OUTLOOK

IDC's forecast for Windows Vista growth suggests that Vista migration within the current installed base will be gradual and very much unlike the launch and migration of Windows 95 more than a decade ago. The total installed base is stabilized around Windows XP, which accounts for more than 90% of the installed base of total Windows client operating environments today. Significant installation within the enterprise installed base is expected to occur during 2007 and 2008. IDC doesn't expect shipments of Windows Vista Business (all SKUs) to exceed shipments of Windows XP until 2009. For more information, see *Worldwide Windows Client Operating Environments 2006–2010 Forecast: Vista Expands Windows COE Market Opportunities But Won't Accelerate Growth*, IDC #203733, October 2006.

Microsoft has made tools available to support the Vista launch and support enterprise migration, including tools for planning and deploying Vista, for determining if the existing hardware must be upgraded to support the new operating environment, and for volume key and system activation. The availability of free Microsoft tools such as the Business Desktop Deployment 2007 Solution Accelerator, which is a collection of Vista migration tools and guidelines, does not mean that existing infrastructure or non-Microsoft tools are no longer required. It should not be simply assumed that these free tools are the optimum Vista migration and ongoing management solution for your organization. Vista migration and ongoing management solutions should be carefully evaluated to ensure that they meet your organization's individual needs in terms of automation, integration, speed of imaging and deployment, secure systems retirement, security, and data and systems protection.

CHALLENGES/OPPORTUNITIES

Challenges to Symantec's solutions include the following:

- ☒ **Many of the migration solutions fall within Symantec's Data and Systems Management Group (DSMG) business unit.** Historically, the message within the company of protection made sense for the Ghost and endpoint security product lines, but this last line of defense tended to get lost in Symantec's broader messages relating to security and antivirus, especially for the consumer markets. Symantec must make clear that it is more than just a backup and security company. Further, Symantec has a strong set of offerings, but because many of the products are separate from each other, multiple consoles must be used collectively to achieve the level of integration needed for the complete migration story to work.
- ☒ **Integration of Altiris.** In January 2007, Symantec announced it had entered into an agreement to acquire Altiris, a system management vendor that provides, among other solutions, a PC management suite. Symantec announced in April 2007 that it had closed on the Altiris acquisition. Although Altiris has a very complementary product line, it is also somewhat redundant with features previously acquired. Existing features within the Ghost product suite for migration and distribution overlap with the same features within the Altiris product line. Symantec can now move forward to supply multiple products to multiple channels, but it will have work to do to ensure that the natural uncertainty of customers about which products will be discontinued, and which products Symantec will move forward with, is addressed.
- ☒ **Reaching the small and midsize enterprise (SME) in a consistent fashion.** Products such as Ghost for imaging and migration tend to be sold at the departmental level and thus require a focused partner network. As Symantec does more to bundle products into a complete solution to solve an IT or a business problem, the company must have both a stronger message with CIOs and senior management and a partner network that is aware of that message for successful sales to SMEs.

Opportunities for Symantec's solutions include the following:

- ☒ **Integration of the Altiris product line.** The Altiris product line includes virtualization and service desk solutions, which Symantec did not possess.
- ☒ **A strong channel with good customer service.** Altiris did a good job of providing larger partners such as Dell with customer support to win deals and keep customers happy. This is a benefit to Symantec as it moves forward with new customers in the integrated Symantec.

CONCLUSION

Given Microsoft's signals and announcements over the years, forward-thinking organizations have been aware of the impending release of Windows Vista for a while. Certainly, issues about when to migrate servers as well as mission-critical applications and processes factored into their overall thinking. Managing clients factored into their thinking as well because IT administrators want to minimize impacts to users whenever changes are implemented to user PCs. The way to minimize change is to ensure that the detailed planning necessary to successfully determine when to migrate takes into account the tools necessary to do so.

IT departments that are now considering migrating to Windows Vista certainly have much to consider when planning and executing the migration, as well as dealing with the post-migration environment and managing that environment effectively. Effective pre-migration planning helps smooth the actual migration and simplifies the environment moving forward. These pre-migration planning activities start with determining if existing PCs are Vista Premium Ready or Vista Capable; if neither, IT departments must determine the required budget and effort to get the PCs into a state to accept the new operating environment. Then IT administrators and managers can focus on the following activities necessary to kick off such an effort:

- ☒ Hardware and software discovery and inventory of PCs
- ☒ How to deploy the new operating environment and other deployment issues
- ☒ Application testing with the new operating environment
- ☒ Data and systems protection and security

These activities lead into the post-migration planning and what the IT department wants its new PC environment to look like. IDC's research has shown that best practices for managing any PC environment should:

- ☒ Minimize the number of different hardware and software PC configurations
- ☒ Standardize and minimize the overall number of tools
- ☒ Automate as much of the process as possible

This leads to downstream benefits of being able to leverage virtualization technologies, evaluate benefits of new and emerging technologies, improve IT governance, and speed delivery of applications through the entire acquisition and test process to end users.

Symantec has released a set of solutions within the existing product line that provide image management, including simplified image editing, rapid and reliable multicast distribution of that image to PCs, comprehensive user migration, and secure system retirement. Symantec's product family can also provide data protection for sensitive corporate data on PCs, both during and after migration, and complete system recovery in minutes in the event of a post-migration failure — even to dissimilar hardware or virtual environments or in remote, unattended locations. And Symantec's brand-name recognition certainly helps credibility when providing a security solution during migration as well as after migration.

Symantec's acquisition of Altiris also has provided Symantec with another set of solutions to manage PC operating environment migrations. The Altiris Client Management Suite is also capable of producing image creation and management, software and hardware discovery and inventory, and distribution of the new operating environment during a Windows Vista migration. Further, the Altiris product family has been augmented over the years with functionality for application virtualization and security, which has delivered a fine set of solutions for consideration. The only items of concern would be how Symantec proceeds with the Altiris acquisition and what the product road map will look like moving forward. Customers interested in what is happening with Symantec's Vista-related products can visit the Symantec Vista Information Center Web site (www.symantec.com/vista), or to the Altiris website (www.easyvistamigration.com) for the latest information.

Symantec fields a comprehensive Windows Protection product suite that can assist in the successful planning and execution of a smooth PC migration to Windows Vista as well as ongoing systems management. IT organizations that are thinking about migrating to Windows Vista should consider Symantec's offerings for their organizations.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2007 IDC. Reproduction without written permission is completely forbidden.