The Road to Desktop Optimization

Five best practices that lead towards an optimized desktop infrastructure

people ready

Introduction

Enterprises worldwide are embracing a digital work style to stay competitive in a dynamic and increasingly global business environment. This work style requires that teams collaborate seamlessly across organizations and time zones, while success relies on speed, mobility and connectivity.

These trends are putting unprecedented demands on IT departments to provide the necessary desktop infrastructure to information workers, enabling a People-Ready Business. The ever increasing need for desktop performance, connectivity and mobility—and the management tools that enable these—add to system complexity at a relentless pace.

The key challenges facing IT managers in this environment can be summarized as follows:

Deployment	Management	Security
• Application compatibility • Numerous software images • Large-scale migration complexity	• Inconsistent configurations • Unpredictable downtime • Decentralized PC management	• Confidential data protection • Security patching • Malware and virus • License compliance

- ***30-45% of IT budget in an average enterprise goes to desktop support***
- ***These pain points drive 20% of desktop TCO and 50% of end-user self-support***

With complexity come greater demands on resources—often outstripping the budget and people available to the IT organization. In addition to pushing up labor costs, system complexity impacts service levels and limits business agility.

What are the stakes? The cost of hardware and software is only a small percent of the total expense to manage a PC—typically 24-28%[1]. The real burden on the IT budget is the labor associated with provisioning and managing PCs across the organization. IDC estimates the annual IT labor cost for maintaining one PC at $1320 in a typical large organization. This same study estimates that an organization that adopts certain best practices that reduce complexity can move this figure down under $230—a reduction of over 80%![2]

Leading companies worldwide are not just coping with these challenges, but are stepping up and turning their desktop infrastructure from a cost center to a *strategic asset*. Microsoft's Infrastructure Optimization model illustrates the varying levels of IT system maturity, and is useful for identifying improvement priorities for individual organizations:

Basic	Standardized	Rationalized	Dynamic
Uncoordinated, manual infrastructure	Managed IT infrastructure with some automation	Managed and Consolidated IT infrastructure	Fully automated management, dynamic resources usage
Cost Center	***Efficient Cost Center***	***Business Enabler***	***Strategic Asset***

[1] *Saving money on PC deployment*, Gartner, Michael Silver, December 8, 2005
[2] *Optimizing Infrastructure: The relationship between IT labor Costs and Best practices for Managing the Windows Desktop*, IDC, #203482, October 2006

The financial impact of moving along the continuum from Basic to Rationalized infrastructure should not be underestimated—nor should the improvement on IT service levels and business agility. IDC conducted a study with 200+ IT departments in the fall of 2006, benchmarking IT costs, service levels and agility. In the case of agility, the metric was how long it takes to deploy a new application or capability. This study found that higher levels of IT maturity resulting in dramatic savings in IT labor, and notable improvements in service levels and application deployment speed.

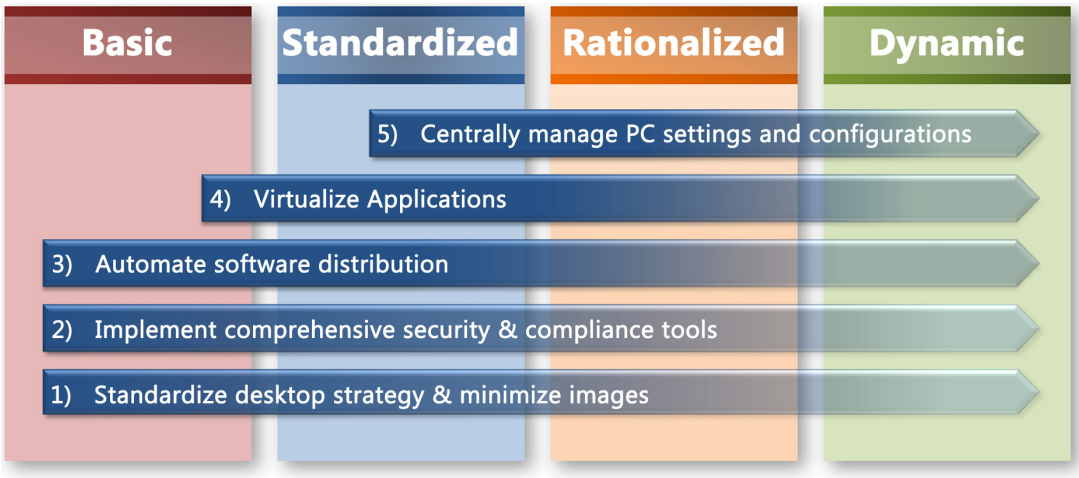
	Basic	Standardized	Rationalized	Dynamic
IT Labor Costs	$1320	$580	$230	*Not Available*
Service levels (#Svc desk calls)	8.4	8.5	7.7	*Not Available*
Business Agility (# weeks/deploy app)	5.4	5.2	4.3	*Not Available*

Source: IDC Core Infrastructure Optimization Research, Summary of Findings Jan 2007

Across top-performing companies, five fundamental practices emerge as critical to moving the IT infrastructure along the maturity continuum—driving down TCO, improving service levels and enabling business agility. These best practices are:

1	**Standardize desktop strategy & minimize images**
2	**Implement comprehensive security & compliance tools**
3	**Automate software distribution**
4	**Virtualize applications and deliver as a streaming on-demand service**
5	**Centrally manage PC settings and configurations**

Combined with the right software tools, well-defined policies and documented processes, these best practices will help you achieve a well-managed, secure IT infrastructure and streamline the efforts to maintain it. To support these best practices, this paper assumes a basic infrastructure is in place for identity and access management, such as Microsoft's Active Directory® directory service.



While each organization has unique attributes that will dictate the sequence of adoption of these best practices, the accompanying diagram illustrates a framework to consider in prioritization

1. Standardize desktop strategy & minimize images

Simplify deployment and provide a more uniform environment

Standardizing on a single hardware platform and operating system, and the resulting reduction in the number of desktop images, is a key first step in simplifying the desktop infrastructure. According to IDC, image management accounts for 20-25% of OS deployment costs, and can cost organizations on average $25-35 per PC annually[3].

From a management perspective, the ideal scenario would be one model of PC, one operating system and the same software loaded on every PC across the enterprise. Historically, this hasn't been realistic given refresh cycles, departmental requirements and legacy equipment. However, new tools are coming available that can provide the same benefits as this monolithic approach, without the overly restrictive hardware and software model. Companies that are able to maintain a standardized desktop realize on **average savings of $110 per PC annually;**[4] bringing this to the point of a single image enterprise-wide would result in even greater savings and IT effectiveness.

The factors driving this improved efficiency are:

- Reduced time testing application compatibility prior to deployment
- Fewer application conflicts, preventing downtime events
- Greater system predictability, resulting in more rapid problem resolution
- Fewer OS environments in which to maintain expertise
- Reduced effort monitoring potential security vulnerabilities

In addition to saving costs, reducing the desktop images managed in the organization will result in higher service levels, as factors that can cause downtime events are reduced and recovery is accelerated. Organizational agility is improved; fewer desktop images make it easier and quicker to deploy new applications across the enterprise.

"Using the imaging technologies in Microsoft Windows Vista would give us a single, standard image we can deploy across all machines and manage and update over the life cycle of each PC,"
Mark Boyd, Team Lead, NSW Dept. of Education

With the introduction of Windows Vista™ Enterprise operating system and Microsoft's Desktop Optimization Pack, organizations can drastically reduce the number of images they must manage. Here's how these technologies address the issue of image management:

Windows Vista Enterprise

- Windows Vista Enterprise employs a new image-management architecture that is hardware independent. Instead of maintaining a separate image for each PC form factor and each hardware design, Windows Vista Enterprise can allow a single image to be deployed across the entire PC spectrum
- Windows Vista Enterprise includes all the Windows user interface languages, allowing IT Professionals to deploy and manage a single, worldwide binary
- LOB applications that have not yet been updated to run on Windows Vista Enterprise can operate in a virtual PC environment on the client PC. Windows Vista Enterprise now provides up to four licenses for prior Windows editions at no additional cost. This eliminates the need to maintain separate images for legacy operating systems

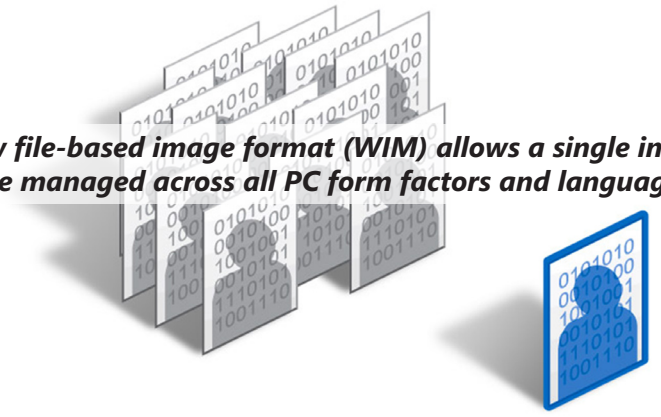
[3] *Ibid.*, IDC, #203482, October 2006
[4] Ibid. IDC, #203482, October 2006

- Microsoft Solution Accelerator for Business Desktop Deployment provides end-to-end guidance for efficient planning, building, testing, and deployment

Microsoft Desktop Optimization Pack (MDOP)

- Microsoft SoftGrid Application Virtualization, available in the Desktop Optimization Pack, separates and isolates the application layer from the operating system. This separation stabilizes the image and allows previously conflicting applications to coexist in the same desktop image, eliminating the need to maintain a unique OS for legacy applications
- Software inventory management and real-time application tracking usage provides a comprehensive view of the desktop environment, streamlining the migration to a single desktop image

In migrating towards a single image across the enterprise, the IT organization enjoys greater simplicity across the ecosystem, a more robust and secure environment, and improved agility. Microsoft Vista Enterprise and Desktop Optimization Pack make these benefits a reality.



New file-based image format (WIM) allows a single image to be managed across all PC form factors and languages

Case Study: New South Wales Department of Education

Customer Size: *160,000 desktop PCs*

Organization Profile

The New South Wales Department of Education and Training, with 1.2 million students and staff at 2,600 schools and Technical and Further Education (TAFE) colleges across the state, is the largest single public or private organization in the country and accounts for a quarter of the NSW state budget.

Business Situation

Although it has made efforts in recent years to standardize its PC fleet, the Department still has many different PCs from a variety of vendors. Including all the different hardware platforms the IT Directorate has to support, there are ***more than 100 images*** *in total, each of which has to be maintained with security updates and other changes. The burden on the IT organization was tremendous, and was a major driver of cost and complexity*

Solution

Starting in August 2006, the Department ran a pilot project at a Sydney high school installing Microsoft Windows Vista on 16 PCs and evaluating the process of creating and deploying standard operating environment images under the new operating system. The result of the pilot was that IT will now be able to manage the infrastructure with a ***single image*** *deployed across every PC.*

Benefits

- *Savings in management time and effort from reducing the number of standard operating environment images*
- *Improved security; less management and helpdesk time*
- *Providing students access to the latest technology to prepare them for further education or the workplace*

2. Implement comprehensive security & compliance tools

Avoid downtime events and quickly resolve them when they strike

Proactive security policies and tools play a key role in maximizing uptime by both avoiding downtime events in the first place, and having procedures in place to resolve the issues quickly and effectively. The most obvious area to address is intrusion from viruses and other malware. Preventing intrusive events from occurring avoids reactive efforts across the organization, and results in lower and more predictable IT labor costs.

IDC reports that organizations with comprehensive security and IT governance tools realized a **typical savings of $130 per PC**[5]. For this analysis, the following aspects of security were considered:

- ✓ Desktops and notebooks were equipped with antivirus utilities and subscription-based updates
- ✓ Desktops and notebooks employed antispyware and malware utilities
- ✓ Notebooks were protected by centrally managed PC firewalls
- ✓ Network Access Control was used for PCs entering the network
- ✓ An automated patch distribution system was in place for all desktops and notebooks

By employing the above security measures, organizations are able to better prevent disruptive occurrences that interrupt user productivity and tie up IT administrators in cleanup activities. For example, by centrally managing the PC firewall settings, IT administrators can rapidly respond to a potential virus attack by closing a particular port on all PCs across the network, rendering the virus inert. If this capability is not available, the subsequent cleanup effort can be very costly. Even if the virus attack fails to penetrate initially, the emergency effort to manually remove the vulnerability would be quite disruptive.

Beyond securing the network and infrastructure, IT needs to ensure that sensitive information is protected from unauthorized access—both while on the network grid and if a laptop is lost or stolen. Several major security breaches have recently been in the news, stemming from the simple mishandling of a laptop.

Compliance and software lifecycle management is a challenge across most enterprises. Some of the issues facing IT managers are:

- Effectively managing the software assets to ensure compliance with licensing agreements
- Optimizing software license expense by ensuring they are allocated to best-use

IT Management Scenario: Application Security Patch

Bill, an IT administrator for a 20,000 seat enterprise, just received notice that a key application used across the company has a critical security vulnerability. A patch has just been released by the application developer, and fortunately none of his PCs have been effected.

Prior to deploying Systems Management Server, Bill would have had to manually get the patch out to every user—either desk to desk, or by relying on individuals to download the patch on their own. Either way, he could never confidently know that the security vulnerability was completely closed.

With SMS in his infrastructure, Bill simply schedules the patch to go out to all of the PCs running this application from one management console. With this tool, he is able to load balance the distribution of the code and plan it for off-peak network use. Within a day, the vulnerability is closed, and Bill has the confidence that each PC that needs the patch has received it. All with just a few clicks of the mouse!

[5] *Ibid*. IDC, #203482, October 2006

- Identifying applications and installations that are contrary to corporate policy
- Analyzing software usage to forecast future organizational needs

As with many IT practices, several of the tools available to efficiently manage the PC infrastructure also aid in security maintenance. For example, an automated software deployment tool that manages the application portfolio also facilitates the automated delivery of patches and updates.

Beyond basic security measures, Microsoft technologies streamline advanced security management and provide IT administrators with visibility into potential vulnerabilities:

Windows Vista Enterprise

- Windows BitLocker™ Drive Encryption in Windows Vista Enterprise provides a robust and automatic method of protecting data in mobile PCs. Unauthorized users are completely locked out if a laptop is lost or stolen
- With Windows Vista, User Account Control allows common user tasks to be performed under a standard user, reducing the incidences where administrator log-in is required. The result is a lower attack surface, and less opportunity for security breaches. Enhanced Windows Security Center increases the security categories monitored beyond internet firewall, Automatic Updates and anti-virus to include malware protection and internet security settings
- Over 500 new group policy objects provide greater management control over security configurations, including disabling USB drives to protect confidential data
- Event Viewer and event logging captures all desktop activities as events. This facilities monitoring for both troubleshooting and regulatory compliance purposes
- Windows Service Hardening restricts critical Windows services from making unauthorized changes in the file system, registry, network, or other resources that could be used to allow malware to install itself or to attack other computers

System Center

- Operations Manager provides enterprise-scale vulnerability awareness, facilitating a proactive assessment of risk through client monitoring. IT management teams can identify and resolve issues before they cause a downtime event. In addition, Operations Manager efficiently supports compliance monitoring
- Configuration Manager sets a configuration baseline for a collection of devices, defined by location, role or use. These baselines can be comprised of OS level, patch level, application presence/version or business rules. Once established, these baselines can then be enforced by policy at regular intervals and used to protect the infrastructure
- Comprehensive patch management automates the delivery of security patches, reducing the duration of vulnerability and lowering implementation cost

Microsoft Desktop Optimization Pack

- Advanced Group Policy Management facilitates a more robust change-control process for group policy objects. Configuration settings for security parameters can be edited and tested offline, then transferred to the live environment without impacting operations
- The Microsoft Diagnostics and Recovery Toolset provides several options for PC recovery if a catastrophic event occurs, even when safe mode or normal boot will not function. An easy-to-use offline boot environment allows recovery of deleted files, elimination of malware, manipulation of services, fast-wipe and more to get the effected PC back up and running
- Asset Inventory Service provides a complete view of the software environment across the enterprise, including Microsoft and third-party applications. With more than 430,000 titles in the database representing the vast majority of commercially available titles, Microsoft Asset Inventory Service helps make sense of the data and provides a perspective anywhere from an enterprise-wide report to an individual workstation drill-down
- Identify applications and installations that are contrary to your corporate policies, and track real-time application usage so you can determine how applications are being used or potentially misused

Managing the infrastructure security in a proactive manner delivers significant savings to the enterprise, both in IT labor savings and maintaining end-user productivity.

3. Automate software distribution

Simply deployment and free up IT resources for higher value work

Transitioning to an automated process and set of tools for deploying new applications is a direct path to IT savings. There are many levels in this best practice, from basic tools that simply push applications to the desktop to comprehensive PC lifecycle management programs. The most obvious benefit is the near-simultaneous delivery to any number of PCs and minimizing the direct intervention by the IT staff or end user. This is particularly important when closing a security vulnerability across the enterprise.

A critical component of this best practice is that the *processes* adopted weigh more heavily than the use of specific tools. To capture the efficiencies and cost savings with automated deployment, an organization needs to develop a robust process around the use of inventories and group targeting, along with software packaging that drives the deployment process.

According to research by Gartner, in a non-automated environment 24% of the variable cost in provisioning a PC involves testing and installing software.[6] The required resources increase dramatically for large scale deployments and upgrades to the operating environment. The cost to provision a single PC **decreases $26 annually** when software deployment automation is adopted, according to analysis by Gartner and Microsoft.[7]

Without an automated deployment process and tool set, the adoption of new IT capability is lengthy, denying the enterprise of benefits they are seeking. Conversely, the adoption of the right tools can allow the enterprise to decouple the deployment of a new operating system from the hardware refresh cycle, accelerating the benefits this migration will yield.

Microsoft System Center with Configuration Manager (formerly Systems Management Server—SMS) allows an organization to streamline the delivery of applications and new operating systems across the enterprise, while providing a greater understanding of the hardware and software infrastructure.

System Center

- Centralization of all deployment tasks from a single management console clarifies the process for network administrators, while the intuitive interface and drag-and-drop capabilities facilitate increased efficiency and operational effectiveness
- Task Sequencer in Configuration Manager streamlines deployment planning and execution, reducing both the resources required and the duration of the effort
- By providing support for client and server deployments in the same process, the overall deployment is simplified, while a common image format with Windows Vista Enterprise reduces system complexity
- For large-scale deployments, offline provisioning allows better control over scheduling, targeting and qualification; load balancing can be managed effectively
- Customization for specific groups is simplified and easily configured. The Driver Library decouples driver configuration from the PC image, reducing potential conflicts and problems

"Across EMEA, we're gaining 180,000 hours a year in improved productivity because of software deployments that are automated by Microsoft technology" *Michael Partsch, Chief Information Officer EMEA, Central Region EDS*

[6] *Saving money on PC deployment*, Gartner, Michael Silver, December 8, 2005
[7] *Infrastructure Optimization*, William Barna/Microsoft, April 2006

Managing software deployment with a set of integrated tools and well-defined processes yields significant resource savings, while accelerating the delivery of capability to the business. In addition, the visibility into the hardware and software ecosystem allows the IT organization to more effectively manage permissions and compliance across the enterprise.

Case Study: EDS Europe, Middle East & Africa (EMEA) Central Region

http://www.eds.com

Customer Size: *30000 employees*

Organization Profile

EDS is a technology solutions provider that offers consultancy and technology support services to corporate and public sector customers worldwide.

Business Situation

EDS required an automated deployment solution to help install business productivity applications and security software updates across its disperse network, including areas with bandwidth limitations. Software deployment costs were high, field penetration of security updates were low due to an end-user centric process, and field service requirements were significant.

Solution

EDS chose a solution based on Microsoft® Systems Management Server 2003, which has dramatically reduced software support costs and improved security compliance throughout the company. This solution administers all security updates, hardware and software inventory, asset tracking, reporting, and software distribution.

Benefits

- *High-quality support for rollout*
- *Central deployment cost reduction*
- *Improved productivity*
- *Enhanced systems security*
- *Optimized bandwidth for deployment of security updates*

Software and Services

Microsoft Active Directory

Microsoft Operations Manager (MOM) 2005

Microsoft Systems Management Server 2003

Microsoft Windows Server 2003 Standard Edition

4. Virtualize applications and deliver as a streaming on-demand service

Reduce application conflicts and increase system uptime

One of the major challenges in managing a desktop infrastructure is avoiding conflicts between the numerous applications found across an organization. Regression testing applications prior to deployment is taxing for IT administrators; the rigorous application compatibility testing required prior to the launch of an operating system upgrade is a major reason most organizations are unable to deploy the latest OS in the time frame their business users desire.

In a traditional model, each PC has an array of applications suited to the individual user. These applications require lengthy regression testing and deployment processes before they reach production. Because applications are only available where they are installed, the applications are tied to a specific computer, and typically a user is coupled with a specific computer. All of this makes migration planning and security management a complex, labor intensive practice.

Microsoft SoftGrid provides a new way to deliver application capability to the end user desktop—as a virtualized, digital-streaming service. By delivering virtualized applications on-demand and separate from the desktop image, several benefits emerge:

1. The reduction of application-to-application conflicts simplifies application portfolio management across the enterprise. Previously conflicting applications can be run on a single PC without incident
2. Application compatibility testing is reduced, lowering resource demands and accelerating OS migrations and application deployments
3. Centralized Policy-based management is more easily administered, and patching can be performed on the common code base. Repairing or updating applications involves a single incidence, rather than every PC in the organization
4. Flexibility is increased as applications are decoupled from desktops, and desktops are decoupled from specific users
5. Compliance is ensured, as permissions are centralized preventing unauthorized use
6. Security is improved as applications can be locked down in read-only mode, and application isolation prevents a potential source for security breach
7. New applications can be deployed across the enterprise more rapidly, improving business agility

Microsoft SoftGrid virtualizes applications per user, per application incidence, without changing underlying source code. The result is a transformed environment with simplified, automated processes for deploying, patching,

IT Management Scenario—Application conflicts from multiple Java VM

Frank is an IT administrator for a major insurance company. His finance department is using several applications that are switching over to be web-based, and use different Java runtime environments. Unfortunately, only a single version of Java can be installed on a client operating system. Because the entire OS is essentially hard coded to a specific Java version, this can prevent other desktop and web applications from functioning correctly. The result was numerous system crashes and a very frustrated finance group.

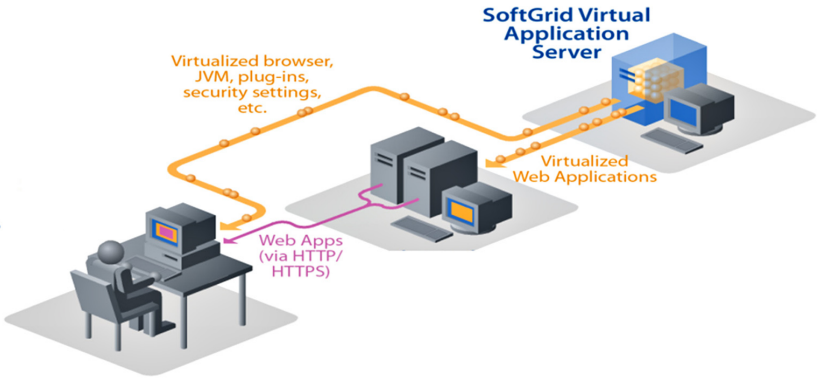
After learning about SoftGrid, Frank ran a pilot program in the finance department to see if virtualizing the applications and delivering them as an on-demand, streaming service was the solution. SoftGrid worked superbly, since it isolated the web applications from the desktop OS—problem solved!

updating and terminating applications, requiring minimal resources and delivering superior results.

"SoftGrid let us quickly turn our entire application environment into on-demand services. This not only saves us significant costs, it also makes us more agile and greatly accelerates our ability to get applications to end users the moment they need them."
Andy Gerringer Senior Network Administrator, Alamance Regional Medical Center

Using Microsoft's SoftGrid-SMS Connector, the combination of SoftGrid with System Center Configuration Manager radically simplifies the deployment and management of the full portfolio of software and applications. With application virtualization, on-demand streaming and self-provisioning, IT administrators are able to push or stream applications across the enterprise from one console—allowing improved control, greater flexibility and ultimately a more optimal desktop infrastructure.

Web-based applications still require local installations—Plug-ins, Java Virtual Machines, Browser Security Settings, Active X controls, Flash, etc. SoftGrid can be used to deliver sequenced versions of web-based applications, so all dependencies (i.e. Java versions, plug-ins, etc.) are self-contained.



Case Study: Alamance Regional Medical Center

***Customer Size**: 2200 employees*

Organization Profile

Alamance Regional Medical Center, which serves central North Carolina, was named by Microsoft Healthcare User's Group (MSHUG) as the 2005 Hospital of the Year for using Microsoft technology to improve patient care quality.

***Business Situation**:*

The IT group managed over 75 applications for 2,200 PC and thin client users. Deploying, updating and supporting these applications were incredibly time-consuming and manual.

- *IT was required to go computer-to-computer to load updates and security hot fixes*
- *215 hours were spent every year on regression testing to ensure applications would not conflict once installed*
- *The mix of desktop and web applications created conflicts stemming from multiple versions of Java VM*

***Solution**:*

Implemented Microsoft SoftGrid application virtualization and dynamic streaming solution to separate the applications from the OS. This eliminated the conflicts across applications and reduced both prelaunch regression testing and overall deployment time.

***Results**:*

- *Saved more than $1.5 million in application management costs over 3-year period*
- *Achieved time-to-payback in 5.4 months*
- *Eliminated over 200 hours of regression testing*
- *Deployed new applications in 1/10th the time; upgraded applications in 4 hours instead of 8 days*
- *Eliminated 5,000 hours of annual end-user downtime, saving $100,000 in lost productivity*
- *Decreased helpdesk call volume by 30%, while resolving issues in half the time*

5. Centrally manage PC configurations and settings

Drive complexity out of the desktop environment and maximize user uptime

One of the highest-return best-practices in regards of IT labor reduction is to centrally manage the configurations and settings on the PCs across the network. IDC estimates that moving to central control will save an **average of $190 per PC annually**.[8]

Taking control of the desktop environment directly leads to greater stability, faster problem resolution and fewer problems with software deployments and patches. This is because reducing the ability for end users to change settings and configurations reduces overall system complexity, and avoids potential conflicts between these settings and the applications you are deploying.

Let's look at these issues one at a time:

1. Many downtime events can be traced to incompatibilities between a newly deployed application and specific settings the PC user has previously made. Locking down a portion of these settings will allow the IT Pro to ensure that the environment an application is being deployed into matches the test environment

2. Reducing variability between PC settings and configurations leads to a more uniform, predictable environment. For technicians at the help desk or those that provide desk side service, understanding what to expect before engaging in problem resolution simplifies the task. This allows quicker problem resolution for shorter downtime duration

3. Maintaining a less complex and more predictable desktop environment also reduces the time needed to deploy an application, as the variables required for testing are reduced. Businesses gain agility, and the IT organization gains confidence that deployment conflicts can be avoided

The challenge the IT organization will face in administering this best practice is that some business divisions might require unique configurations to support specific needs or

"We are now in a position to increase our number of employees by up to 30 percent and still support the organization with the same infrastructure" *Gabriel Pepe, Distributed Systems Director, HSBC Mexico*

LOB applications. Similarly, some end users might need to make modifications to optimize a system to their personal needs. To a great extent, these issues can be addressed with the right management tools.

A key component of centrally managed settings and configurations is controlling the software that gets loaded on PCs, avoiding immediate and subsequent problems.

- Application conflicts can be identified and avoided prior to software getting loaded onto a PC. An individual user typically does not have the tools or knowledge to properly assess interoperability, and may not use appropriate caution when adding software

- Problem resolution is accelerated since the IT administrator or help desk approaches a known application environment, and the variables he or she must contend with are reduced

Microsoft offers several technologies designed to streamline the centralized management of the PC environment:

Windows Vista Enterprise

- Group policy reach is extended to over 500 objects, including power management settings that allow administrators to save on electrical consumption and control over external device connections

- User Account Control reduces the need for users to work in an administrator mode, so standard users are prevented from making potentially dangerous changes to their computers

[8] *Optimizing Infrastructure: The relationship between IT labor Costs and Best practices for Managing the Windows Desktop*, IDC, October 2006

- Event Viewer and logging makes the Windows Vista Enterprise desktop easier to manage and monitor, and provides better information for troubleshooting. Every desktop activity is captured as an event, providing a self-documenting environment for regulatory compliance reporting

- Wherever possible, Windows Vista will heal itself, avoiding user interruptions and unnecessary help desk calls. If Windows cannot fix the problem automatically, built-in diagnostics log when a system error takes place and may walk the user through solving the problem

System Center

- Configuration Manager enables group policy-based administration, simplifying operations and policy enforcement through an easy-to-use console. Drag and drop capabilities and an intuitive interface reduces the complexity of systems management

- Operations Manager provides a comprehensive view of health of the IT environment, delivering end-to-end service monitoring while automating routine, redundant tasks

- Service Desk further automates problem resolution with a comprehensive diagnostic toolset while integrating routine monitoring and reporting tools

Microsoft Desktop Optimization Pack

- Advanced Group Policy Management (AGPM) increases administrators' control of group policy objects, providing a more robust environment for managing GPO changes. Modifications can be made in an offline mode, with differences between live, archived and working versions available for analysis to identify conflicts prior to deployment

- AGPM provides role-based delegation, allowing administration tasks to be delegated to regional or task-oriented administrators. An optional review and approval workflow process prior to live deployment increases management control

- SoftGrid Application Virtualization facilitates the centralization of all application permissions, aiding in governance and compliance

By producing a predictable, uniform environment and eliminating potential problems before they occur, centrally managing PC settings and configurations is a major step towards reducing overall IT costs and freeing up talent to higher-value use.

Case Study: HSBC Mexico

HSBC

Customer Size: *25000 employees*

Organization Profile

Grupo Financiero HSBC has 22,400 employees and 1,400 branches throughout Mexico. HSBC Mexico offers its six million customers a range of corporate and personal financial services.

Business Situation

HSBC Mexico wanted a solution that would help standardize IT operations and support business growth through automated application deployment and improved asset management. Following a 2002 acquisition, the company faced a decentralized IT environment, without a consistent method of software distribution and patch management. IT staff could respond to changes affecting system integrity and security only after they occurred, and HSBC Mexico had difficulties responding quickly to market demands

Solution

The financial service company chose a management solution based on Microsoft® Systems Management Server 2003, Operations Manager 2005, and the Active Directory® service to improve control of its IT environment. First, the company consolidated scattered departmental servers into a central data center. Next they standardized on Windows Server 2003 for servers and Windows XP for workstation. The automated installation process proceeded quickly; at one point using Systems Management Server, they were able to provision 20 branches and 300 workstations in a single day. Eight months later the deployment was complete. Now the company can automatically install updates, get new financial service software to market quickly, and cut IT travel costs. It can also monitor systems in real time and plan for change and business growth.

Benefits

- Remote management cuts costs, reduces time-to-market
- IT environment changes from reactive to proactive
- Better system management supports business growth

Software and Services

Microsoft Active Directory

Microsoft Operations Manager (MOM) 2005

Microsoft Systems Management Server 2003

Achieving Desktop Optimization

Employing these best practices across your company with Microsoft Windows Vista Enterprise, Microsoft Desktop Optimization Pack and System Center will move your organization closer to Infrastructure Optimization

- ✓ Complexity will be reduced, with IT administrators encountering a more uniform, predictable environment
- ✓ Stability will be increased as potential problems and security breaches are eliminated or controlled
- ✓ Flexibility will improve, increasing the ability of IT to quickly respond to needs of the business
- ✓ Automation will increase the productivity of the IT staff, reducing routine tasks and freeing them up for higher-value purpose
- ✓ Downtime will decrease, and potential service interruptions are eliminated and incident resolution is accelerated
- ✓ Compliance will increase and become more automated
- ✓ Operational Efficiency increases providing better service levels with lower IT labor

Microsoft Technologies covered in this paper:

Windows Vista Enterprise	Microsoft Desktop Optimization Pack for Software Assurance	Microsoft System Center
Designed to lower desktop costs, improve security and empower workers with smart information management tools, advanced mobility and secure connectivity	*A dynamic desktop management solution for Software Assurance that provides powerful tools for optimizing the PC infrastructure*	*The comprehensive suite of infrastructure management tools that complement Windows server and client platforms*
• Easier and faster access to information with a new, more **efficient user interface**, while integrated search and new ways to organize files helps you find, use and share information	• SoftGrid Application Virtualization enables applications to run as network services, **reducing conflicts** and minimizing images	• Operations Manager provides end-to-end service management for **intelligent monitoring and reporting—**helping you increase efficiency while enabling greater control of your IT environment
• Windows BitLocker™ Drive Encryption provides **enhanced Data protection** for mobile PCs, and offers complete protection when decommissioning PCs	• Asset Inventory Service provides an enterprise-wide software inventory, with real-time application usage, enabling IT to better manage and **control the software environment**	• Configuration Manager drives IT productivity by **reducing manual tasks** in software provisioning, configurations, patching and asset management
• Access to all worldwide Windows interface languages enables organizations to build a **single deployment image** that can be used worldwide	• Advanced Group Policy Management **increases administrators' control** over desktops, with full change-management tools and offline editing	• Data Protection optimizes and speeds disk-based back-up and recovery, providing bear **continuous data protection**
• Built-in tools to improve **application compatibility** with previous versions of Windows and UNIX operating systems	• Diagnostic and Recovery Toolset provides troubleshooting tools to **pinpoint problems**, recover and repair PCs, and conduct post-crash analysis	• **Capture and aggregate knowledge** about your infrastructure, policies, processes and best practices

For more information on the Microsoft technologies discussed, contact your Microsoft Account Manager or please see the following websites:

Windows Vista Enterprise
www.windowsvista.com

Microsoft Desktop Optimization Pack
www.windowsvista.com/optimizeddesktop

Microsoft System Center
www.microsoft.com/system center