

# The Road to Desktop Optimization

Five Best Practices for Optimizing the Desktop Infrastructure



# Introduction



**...knowledge workers** could more securely access their data and applications from anywhere; whether from their laptop at a customer site; on a shared PC at the branch office; or a non-company PC at home or on the road.

**...office workers** had the flexibility to run their productivity applications on their desktop computers, while seamlessly accessing line-of-business applications running on a secured central server.

**...contractors or offshore workers** could run the latest powerful applications on older, less capable PCs while their data is kept in controlled, central locations.

**...your organization's** desktop infrastructure provided the power and flexibility needed by end-users, while improving the security and control required by IT.

## Desktop Optimization: Achieving Both Flexibility and Control

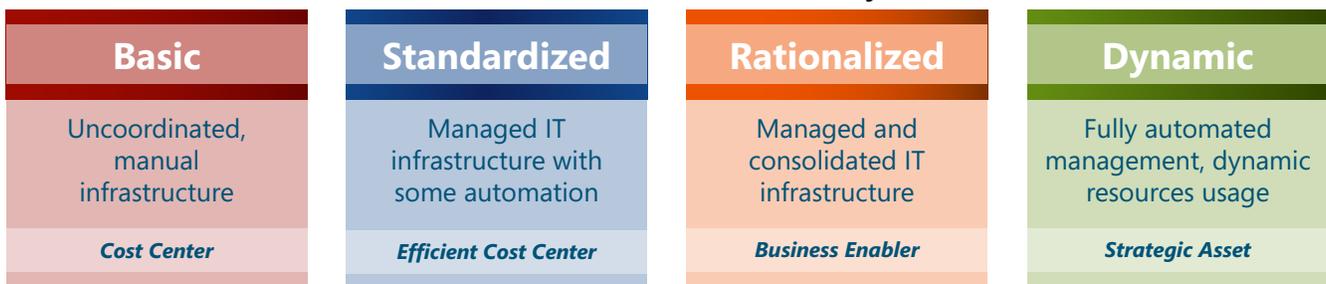
For many organizations, the scenarios above may seem difficult to achieve—if not unattainable. However, the fact is that organizations today have gone beyond imagining these scenarios. They have made them a reality. What these scenarios describe is the working environment made possible by desktop optimization. Desktop optimization means that an organization has attained the right balance in its desktop infrastructure—empowering employees with the flexibility they need to be productive, while providing IT the needed level of control, manageability, and security.

Desktop optimization creates significant organizational benefits. Employees can be more productive with access to applications and data on demand—virtually wherever, whenever they need them. Information and systems are well-protected, better supporting compliance needs with comprehensive security and increased control. Desktop deployment, management, and support are dramatically simplified through virtualization, automation, and centralized administration. Ultimately, desktop optimization is about providing an infrastructure that helps organizations control costs, improve systems availability, and enable greater business agility.

## The Roadmap to Desktop Optimization

Critical to success in achieving desktop optimization is a roadmap that defines and prioritizes concrete steps to advancement. The Microsoft Core Infrastructure Optimization (Core IO) model provides that roadmap. The Core IO model helps organizations to evaluate their placement on a progression of four IT maturity levels from “Basic” to “Dynamic” (see chart) and provides a complete set of guidance, tools, and resources to help advance through the levels toward greater desktop optimization.

**The Core IO Model for IT Maturity**



Thousands of organizations are currently using Core IO to advance along the continuum from Basic to Dynamic IT infrastructure, and the benefits are well-documented. IDC conducted a study with over 200 IT departments in the fall of 2006, benchmarking IT costs, service levels, and “agility”—defined as how long it takes to deploy a new application or capability. This study found that higher levels of IT maturity resulted in dramatic savings in IT labor and notable improvements in service levels and application deployment speed.

The Organizational Benefits of Core IO (\$US)

	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

The State of Indiana estimates it has saved more than \$14 million, including \$6 million in reduced support costs from infrastructure optimization.

<http://www.microsoft.com/casestudies/casestudy.px?casestudyid=4000001697>

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

### Five Best Practices for Desktop Optimization

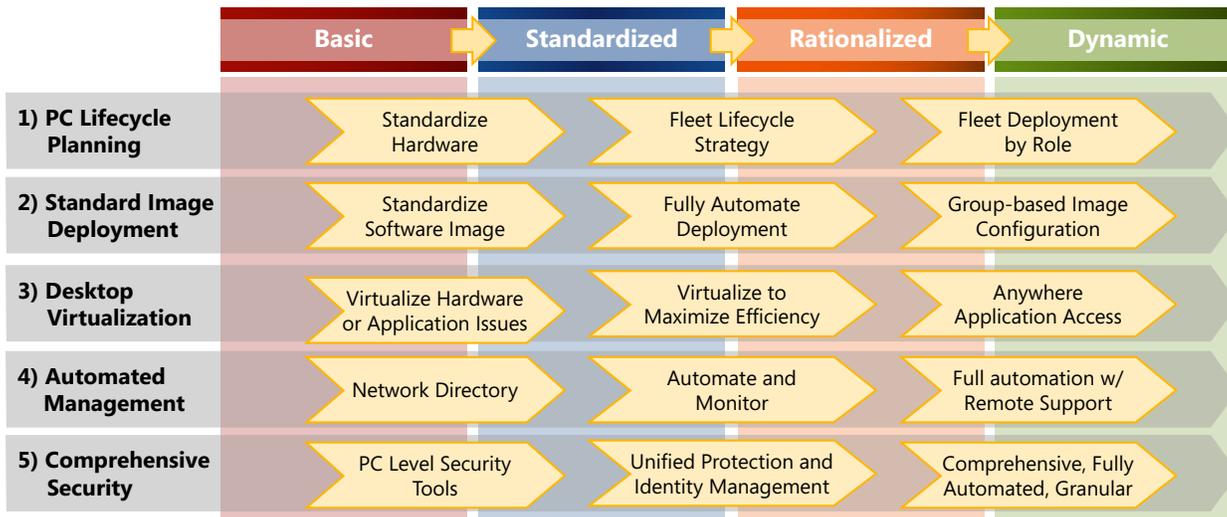
To achieve an optimized desktop, organizations combine technology and practices, specific repeatable methodologies, procedures, and policies that put their technology into action. Across top-performing companies, five fundamental practices emerge as essential to moving the IT infrastructure along the maturity continuum.

### Best Practices for Desktop Optimization

- 1 PC Lifecycle Planning
- 2 Standard Image Deployment
- 3 Desktop Virtualization
- 4 Automation of IT Management
- 5 Comprehensive Security

Each organization will have its own unique path for achieving these best practices; the accompanying diagram illustrates a high-level view of the progression steps within each best practice.

Advancing Core IO Maturity through Desktop Optimization Best Practices



In this paper, we will examine each of these best practices and provide links to specific guidance on how to advance toward greater desktop optimization from each of the Core IO maturity levels. But first, we will take a closer look at some of the “Imagine” scenarios from the introduction and see how desktop optimization can empower organizations to be more productive through greater IT flexibility and control. Beyond cost savings, improved service levels, and increased agility, the user productivity gains exemplified by these scenarios can dwarf the directly measured benefits of desktop optimization.



## Imagine if... Flexible User Scenarios Enabled by Desktop Optimization

In any organization, it is the people that drive business success. Today's organizations look to the IT department to build and manage an infrastructure that supports and enables people to be successful in their jobs. Often, this creates a natural tension between end-users who want the flexibility to support a dynamic work environment and an IT department that needs greater control and manageability. ***Here we will examine five common user scenarios that illustrate how desktop optimization can empower people to do their jobs more productively, while providing a greater level of control and manageability to IT.***

### Streamlined PC Management and Compliance for Increased On-site Productivity



#### Task Worker Scenario

Task workers, such as call center employees, warehouse workers, or retail employees, typically use a single application throughout their day. These workers need the flexibility to access their applications and data from any desk within their workplace. The IT department needs to ensure that confidential data never leaves the data center, improving compliance and limiting risk of data theft.

For task workers, IT can extend the life of older laptops by providing remote access to applications using Windows® Fundamentals for Legacy PCs and Windows Server® Terminal Services. With the application run remotely on the server, task workers can access data and work in the application even though the local PC doesn't have the computing power to run the program itself. With Microsoft® System Center, IT can configure workstations based on a scoped policy, only installing applications specific to the tasks required, and keeping licensing and support requirements to a minimum.

Standardized



#### Office Knowledge Worker Scenario

Many office-based knowledge workers need the flexibility and rich user experience offered by a local desktop PC but with the ability to "roam" elsewhere in the organization, using PCs in different locations to access their own data and applications. These needs can be met using a process known as "hot desking".

With "hot desking," knowledge workers can simply log on to another PC and access their computing environment, including their desktop wallpaper, applications, and files. They have their applications, such as Microsoft® Office Professional 2007, delivered to their desktops using Microsoft Application Virtualization. Using Folder Redirection, data is saved to a central server for regular backups and improved security. Centrally managed programs such as line-of-business applications can be accessed via Windows Server® 2008 Terminal Services, which helps to protect the data and keeps it from being sent across the network (which may be required to meet compliance needs). With Microsoft® System Center, IT can ensure that the right virtualized applications are installed, and customized based on user rules.

Rationalized

## Secure Access to Information Anywhere

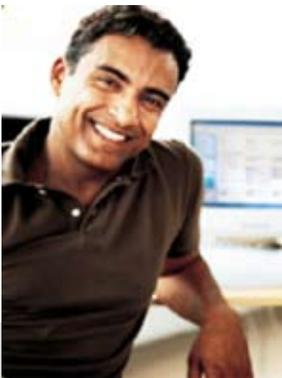


### Mobile Information Worker Scenario

For most organizations, the need for mobile computing is becoming an essential part of the IT infrastructure. Workers today expect flexibility and mobility, and the IT department needs to make sure that data is protected and productivity is not significantly impacted in the case of a lost or stolen laptop. In the “replaceable PC” scenario, mobile workers who lose their laptop can log in to another PC and find their desktop and settings exactly as they left them, with negligible downtime. All of their applications are still available, and they lose no productivity because of the lost laptop.

The Microsoft solution for the “replaceable PC” uses Microsoft Application Virtualization (formerly SoftGrid) to deliver applications virtually to the end-user’s laptop. With Folder Redirection, mobile workers’ data is saved to a central server, so that it will be easily accessible and regularly backed up by IT. If the laptop is ever lost or stolen while traveling, the data is protected by Windows BitLocker Drive Encryption™ (a part of Windows Vista® Enterprise). With Forefront™ Client Security, the desktop is protected against viruses and spyware infecting the operating system. Using Microsoft® System Center, IT can deliver applications – completely installed and configured – based on user profiles, so the user can access them whether connected or disconnected.

Rationalized



### Contract/Offshore Worker Scenario

Organizations that hire contract and offshore workers must protect sensitive data while dealing with unmanaged, non-corporate PCs on their networks. To address this need, organizations can provide virtual access to Windows Vista® on less capable laptops. This enables the IT department to deliver PCs for off-site work while maintaining the data on protected local servers. In addition, they can extend the life of aging PC hardware or deliver a virtual corporate desktop to contractor’s PCs.

For contract and offshore workers, organizations can equip older PCs with Windows® Fundamentals for Legacy PCs (WindowsFLP). Even for laptops without enough RAM to run Windows Vista, an organization can enable end-users to connect to a Windows Vista virtual machine using the Remote Desktop Protocol. With Forefront Client Security, the older PC is better protected against viruses and spyware infecting the operating system. When users log in, they get the entire Windows Vista desktop experience, along with applications such as Office 2007 delivered with Microsoft Application Virtualization. Using System Center, IT can manage the provisioning of virtual desktops hosted in the organization’s data center, allowing access to corporate resources required for these remote workers.

Rationalized



### Anywhere Access Scenario

Employees who work from home or are not able to get to the office need access to their personalized PC work environment, including applications and data, from virtually any location, over the Internet. At the same time, the IT department needs to ensure that corporate data remains protected and that the computing environment remains well controlled.

With Windows Server® 2008 Terminal Services Gateway, the administrator can offer users access to their desktop, applications, and data via Windows Vista® Enterprise Centralized Desktop (VECD) and a remotely accessible Windows Vista virtual machine running on top of Windows Server® 2008 Hyper-V. This access can be made available from the Internet through Microsoft® Internet Explorer® on any PC running Windows Vista® with Service Pack 1 or Windows® XP with Service Pack 3. With System Center, IT can ensure that end-users’ data is replicated when they require a Terminal Services session to work remotely. It also provides application installation and configuration to provision a Terminal Services session nearly identical to the user’s regular office-bound desktop. Using home use rights of Forefront Client Security, employees can install the agent to protect their home PCs against viruses, spyware and other malicious threats.

Rationalized

Now let’s explore how to achieve these scenarios through Desktop Optimization. We will review each best practice in turn.



## Best Practice 1:

# PC Lifecycle Planning

Plan for an optimized fleet strategy across the PC lifecycle

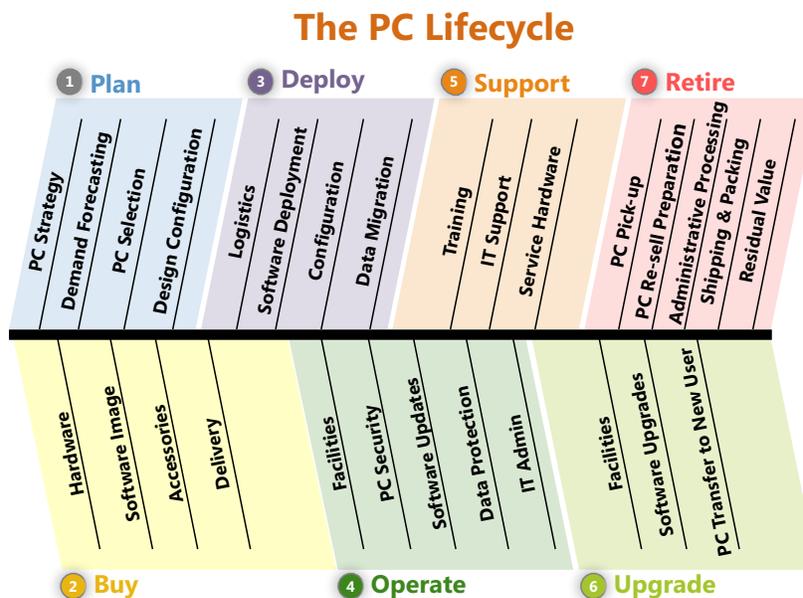
A standardized PC infrastructure forms the foundation for desktop optimization. It is by standardizing desktop hardware and software that organizations can ultimately advance toward a more flexible, agile, and optimized infrastructure. Ad hoc PC purchases—often driven by price, or by departmental and end-user preferences—can ultimately prove much more costly to the organization when a comprehensive view of PC lifecycle costs is taken into account. When the entire span of the PC lifecycle is viewed as a whole, from purchase through retirement, it is clear that purchase price is just one component of PC lifecycle costs.

### Standardize PC Procurement

The first step toward desktop optimization is to standardize the PC fleet hardware to a manageable number of models and configurations. As we will read later in this paper, standard hardware enables standard images and software, which enable standardized testing,

deployment, updating, and support—providing the foundation for automating desktop management. Since it is unrealistic to replace the whole PC fleet at once, it is best to start with standardizing new PCs purchased. IT can use hardware inventory management tools to assess diversity level of the installed base, monitor standardization, and address exceptions. Initially, attrition can be used to move out diverse PCs. The remaining older machines can then be targeted for replacement with new PCs or by transitioning existing standard PCs no longer in use.

PC standardization is best achieved when buy-in is obtained from other departments. The IT department should work with Accounting and Procurement to educate them on the cost savings that standardization can create across the span of the PC lifecycle. IT should then work with Procurement to select a small set of PC hardware options (desktop and laptop)



### Basic → Standardized

#### Standardize Hardware

- Create awareness of the cost of PC diversity to mandate standardization of PC procurement
- Create a long-term plan for fleet standardization to accommodate refresh schedules
- Use asset management software to monitor the diversity of PC hardware and OS on the network
- Target non-standard machines for replacement

#### Benefits

- IT labor savings - \$110/PC/yr from reduced testing, image management, and help desk specialization
- Purchasing leverage
- Reduced spare parts inventory

#### Implementation Guidance

- Core Infrastructure Optimization Implementer Resource Guide: Basic to Standardized <http://www.microsoft.com/downloads/details.aspx?FamilyId=77C0EA3A-BC82-456C-B13D-CFC04D9DCB89&displaylang=en>
- Microsoft PC Lifecycle White Paper 2008
- "Optimizing Infrastructure: The Relationship Between IT Labor Costs and Best Practices for Managing the Windows Desktop," IDC, #203482, October 2006
- Recommended Practices: Strategic Management of the PC Installed Base, Wipro, Order number: 303149-001US, 2004

### Standardized → Rationalized

#### Fleet Lifecycle Strategy

- Analyze costs across the PC lifecycle to assess full impact of fleet strategy decisions, e.g. refresh rate, laptop vs. desktop, HW capability, PC re-issue
- Understand how OS and PC management tools impact cost elements
- Share cost analysis with business groups to assess preferred service level vs. cost tradeoff

#### Benefits

- Reduce PC lifecycle costs within and beyond IT, e.g.
  - Electricity savings with power management
  - Reduce retirement cost with disk encryption
  - Reduce upgrade cost with USB upgrade
- Improve service level / cost tradeoffs

#### Implementation Guidance

- Core Infrastructure Optimization Implementer Resource Guide: Standardized to Rationalized <http://www.microsoft.com/downloads/details.aspx?familyid=ED8F8C4A-5E48-46BA-89B6-17D9F8894AB5&displaylang=en>
- Windows Springboard Implementation Guide – "Improving System Resiliency, reliability, and Hardware Performance" <http://technet.microsoft.com/windows>
- Core IO – Automated tracking of hardware and software assets for desktops <http://technet.microsoft.com/library/bb821285.aspx#EIAA>
- Core IO – Windows XP SP2 or newer operating system <http://technet.microsoft.com/library/bb821285.aspx#EHA>
- Microsoft PC Lifecycle White Paper 2008
- Alinean ROI Tool <https://roi analyst.alinean.com/microsoft/iotool/launch.html>

for the businesses to choose from, and establish an IT policy of only supporting standard PCs going forward. Likewise, Accounting should establish policies approving only purchases of the standardized models.

### Map Total Cost of Ownership (TCO) across the PC Lifecycle

A key component to standardization is to define and articulate TCO for the complete PC lifecycle—from planning through retirement. A full view of the PC lifecycle and related costs enables longer term planning in order to optimize complex fleet management decisions, such as refresh frequency, laptop vs. desktop, hardware capability level, re-issuing used PCs, and role-based use scenarios. This also creates the opportunity to identify immediate cost benefits. For example, an average desktop PC and monitor, left on, will consume \$400 of electricity over a four-year lifecycle. This cost can be significantly reduced by standardizing power management configuration in the PC operating system. However, without a comprehensive PC fleet strategy focused on optimizing the entire PC lifecycle, awareness of these types of costs is often limited.

### Standardization as the Foundation for Future Flexibility

Desktop standardization fundamentally enables the decoupling of hardware from software at the operating system level, creating the possibility for virtualization, automation, centralized management and deployment, as well as other optimization capabilities. Ironically, it is standardization that ultimately provides IT organizations the flexibility to adapt the PC infrastructure to meet changing organizational and end-user requirements. Standardization is the first step toward a more powerful,

dynamic desktop infrastructure, with capabilities such as zero-impact PC hardware upgrades, automated configuration management, and delivery of hardware-independent applications as dynamic real-time services.

### Key Benefits

Standardizing and managing PCs as a fleet, with consistent policies and practices, enables the enterprise to benefit from its scale. With a consistent approach to fleet management, organizations can achieve numerous benefits:

**Effective PC fleet management** – Understanding PC lifecycle costs leads to better fleet strategy decisions, such as prioritization of investments and optimal configuration choices. By managing the PC fleet as a whole, the value of these decisions can be leveraged across the entire enterprise.

**Reduced cost of IT complexity** – As hardware configurations grow, so do costs. A 2004 study found “On average, each additional hardware configuration introduced into a desktop environment results in a \$12 increase in yearly support costs for each desktop PC.”<sup>1</sup> An optimized PC fleet management strategy helps to reduce the complexity of deployment, asset management, system monitoring and software updates.

**Adaptable PC Infrastructure** – System flexibility allows a repurposing of hardware to meet the needs of different roles and business needs across the organization.

<sup>1</sup>Wipro 2004, “Recommended Practices: Strategic Management of the PC Installed Base” (Sponsored by Microsoft and Intel)

## Rationalized → Dynamic

### Fleet Deployment by Role

- Upgrade/replace hardware without downtime
- Re-deploy aging PCs to task- and offshore workers
- Easily deploy cost-effective specialized and/or application-dedicated PCs

### Benefits

- Boost productivity and improve flexibility by better matching hardware and refresh cycle to user needs
- More easily re-use/repurpose older hardware to extend the value of every PC investment

### Implementation Guidance

- Core Infrastructure Optimization Implementer Resource Guide: Rationalized to Dynamic <http://www.microsoft.com/downloads/details.aspx?familyid=03057E09-64F6-4AFF-89C4-D842020A427E&displaylang=en>
- Windows Optimized Desktop Scenario Videos <http://www.microsoft.com/windows/products/windowsvista/enterprise/default.msp>
- Windows Springboard Implementation Guide – “Remote Management of Laptop PCs” <http://technet.microsoft.com/windows>

## City of Zurich



### The City of Zurich Simplifies Management by Standardizing

#### Situation

The City of Zurich is optimizing its IT infrastructure by bringing its 15,000 PCs and notebooks spread across 60 service departments in line with one common standard.

The City decided to standardize on Windows Vista® and the 2007 Microsoft® Office system.

The standardization reduces administrative costs, enhances security, and simplifies the task of locating and fixing errors.

#### Results

*“The City of Zurich is using Windows Vista and Office 2007 to modernize its desktop workstations... With Windows Vista and Office 2007 as a basis, we can offer our customers solutions in no time at all...”*

**Daniel Heinzmann**  
Director, IT Service Department  
City of Zurich

<http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000001326>

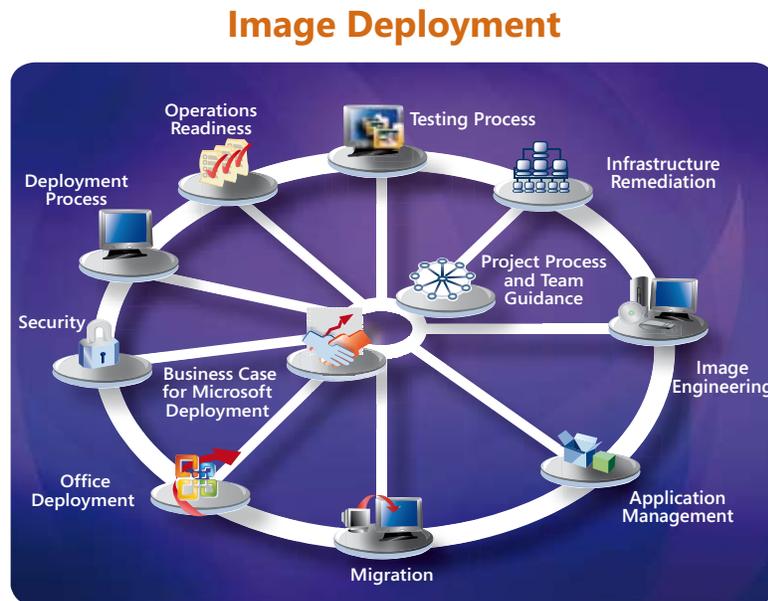
## Best Practice 2:



## Standard Image Deployment

*Deploy standardized images centrally with zero touch to reduce complexity*

After standardizing desktop hardware, the next step toward reducing complexity and optimizing the desktop infrastructure is to standardize the software image. According to IDC, image management accounts for 20-25% of operating system deployment costs, and can cost organizations on average \$25-35 per PC annually. With multiple images, deployments are more time consuming, requiring more manual tasks to accommodate a variety of hardware and software configurations throughout the enterprise. Furthermore, with non-standardized environments, application compatibility can be a much greater challenge, leading to additional time and cost for testing, troubleshooting, and remediation of application conflicts.



In contrast, with a standard software image, IT has the foundation for fully automated “zero-touch” deployments, dramatically reducing the number of manual steps needed to deploy software and freeing up IT time to focus on exception handling. Consolidating to one or two images that can be dynamically updated dramatically accelerates the IT department’s business responsiveness, with lower software costs, reduced testing, improved uptime, and reduced support.

### Create a Standard Image for New PCs

The first step is to create a standard image for use by all new PCs added to the infrastructure. The new image should be made available for installation, whether it is pre-installed by an OEM or a “wipe and reload” is performed by the IT department. To determine what should be

#### Basic → Standardized

##### Standardize Software Image

- ☑ Define and install a common image on all new PCs
- ☑ Encourage user groups to “opt-in” to standard image for service level gains and reduced costs
- ☑ Manage toward standardizing applications and a single image across the enterprise
- ☑ Maintain the standard image (updates, patches, etc.)
- ☑ Use network update to keep standardized PCs in synch

##### Benefits

- Foundation for automated patching and updates
- Lower help desk and image management costs
- Reduce risk and improves compliance
- Increase IT responsiveness
- Reduce impact on end-users for updates

##### Implementation Guidance

- Core IO – Defined set of standard basic image <http://technet.microsoft.com/library/bb821257.aspx#EHAA>
- Core IO – Maximum of two OS versions for client PCs <http://technet.microsoft.com/library/bb821257.aspx#EBAA>
- Windows Springboard Implementation Guide – “Group Policy Configuration Management to Reduce Help Desk Calls” [http://technet.microsoft.com/windows.com/en-us/library/bb821257\(TechNet.10\).aspx](http://technet.microsoft.com/windows.com/en-us/library/bb821257(TechNet.10).aspx)
- Microsoft Deployment – Getting Started [http://technet.microsoft.com/en-us/library/bb891786\(TechNet.10\).aspx](http://technet.microsoft.com/en-us/library/bb891786(TechNet.10).aspx)

#### Standardized → Rationalized

##### Fully Automate Deployment

- ☑ Reduce to one or two standard OS images
- ☑ Perform zero-touch image wipe and reload for:
  - Deployment, whether to one or thousands
  - Transitioning PCs to new users
  - Delivering help desktop solutions
- ☑ Implement Group Policies to prevent non-sanctioned user configuration and software

##### Benefits

- Enable update to modern OS
- Reduce help desk and testing support costs
- Boost service levels by avoiding application conflicts
- Improved control and security

##### Implementation Guidance

- Core IO – Automated operating system image deployment to desktops <http://technet.microsoft.com/library/bb821285.aspx#EJAA>
- Core IO – Layered or thin image strategy for desktops <http://technet.microsoft.com/library/bb821285.aspx#EAAA>
- Core IO – Office 2003 or newer productivity software <http://technet.microsoft.com/library/bb821285.aspx#EGAA>
- Windows Springboard Implementation Guide – “Advanced Desktop Management Approaches” [http://technet.microsoft.com/windows.com/en-us/library/bb821285\(TechNet.10\).aspx](http://technet.microsoft.com/windows.com/en-us/library/bb821285(TechNet.10).aspx)
- Windows Springboard Implementation Guide – “Security Hardening & Defense-in-depth” [http://technet.microsoft.com/windows.com/en-us/library/bb821285\(TechNet.10\).aspx](http://technet.microsoft.com/windows.com/en-us/library/bb821285(TechNet.10).aspx)

included in a standard image, IT should gather information from multiple sources, to include determining the software (including drivers) needed for the PC to function; taking an inventory of the software currently on the network; and working internally with business units, local IT resources, and end-users to understand what software is necessary.

### Transition toward Broad Adoption of the Standard Image

The next step is to create an “opt-in” policy and promote the benefits of standardization to the organization, making business users aware of benefits such as improved system uptime and more responsive support for standardized groups. As the organization becomes increasingly standardized, the reduced cost of support, and the benefits of zero-touch patch and update deployment become more apparent throughout the organization.

### Implement Group Policies to Maintain Infrastructure Standardization

With a standard image in use, IT organizations can centrally implement Group Policies help that prevent unwanted configurations and software installations. With the ability to perform advanced Group Policy management, IT can better ensure that desktops remain in compliance with defined standards and are optimized for ease of maintenance, improved application compatibility, and optimal security.

### Handle Advanced Scenarios Dynamically with One Image

Ultimately, advanced image management can be used

to achieve the highest levels of organizational flexibility. With an advanced operating system, one image can support multiple hardware configurations. Non-standard software can be handled outside of the standard image and virtualized for “on demand” delivery over the network. Furthermore, advanced image management allows specific software to be dynamically tailored for individual PCs and users based on the groups to which they belong (for example by language, geography, role, function, or level).

#### Key Benefits

A key step toward desktop infrastructure optimization, standardizing the software image result in to the following significant benefits to the organization:

**Reduced IT Support Costs** – By enabling greater automation and increasing efficiency, a standardized software image helps to reduce costs for deployment, image management, and ongoing patches and updates.

**Improved Application Compatibility** – Organizations can reduce the time and costs associated with application compatibility issues and testing by reducing conflicts and increasing control over desktop configurations.

**Improved IT Service Levels** – Increased automation and more centralized control helps IT improve service levels by more quickly deploying patches and updates, and reducing potential conflicts from non-standard PC configurations.

## Rationalized → Dynamic

### Group-Based Image Configuration

- Automate management of modular OS images/ applications to tailor image by groups (e.g. function, language)
- Store and manage hardware-specific installation variables outside of the OS image
- Use single-image deployment to extend high service levels without linear increases in cost

#### Benefits

- Increased fully-automated deployments
- Faster deployment and support of new and different hardware types
- Increased application installation flexibility

#### Implementation Guidance

- Windows Springboard Implementation Guide – “Meet Emerging Compliance and Governance” <http://technet.microsoft.com/windows>
- Windows Springboard Implementation Guide – “Remote Management of Laptop PCs” <http://technet.microsoft.com/windows>

## PCL Constructors Streamlines Deployment Process



### Situation

PCL wanted to conduct an enterprise-wide upgrade to the Windows Vista® operating system and the 2007 Microsoft Office system — with minimal disruption to its business.

To solve some of its deployment requirements, PCL turned to Windows® Deployment Services (WDS), a feature of Windows Server 2008.

Through WDS, end users’ workstations are upgraded more quickly with fewer issues, so users can come into the office and get right to work following a deployment.

### Results

*“We were stuck as to how we could rapidly deploy Windows Vista on 50 to 100 desktop computers at the same time...With Windows Server 2008, we had the means to successfully achieve our goal of performing quick weekend and overnight deployments...So far, we’ve used Windows Server 2008 to successfully deploy about 1,000 workstations.”*

**Chris Palmer**  
Senior Server Architect  
PCL Constructors

<http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000001429>

## Best Practice 3:



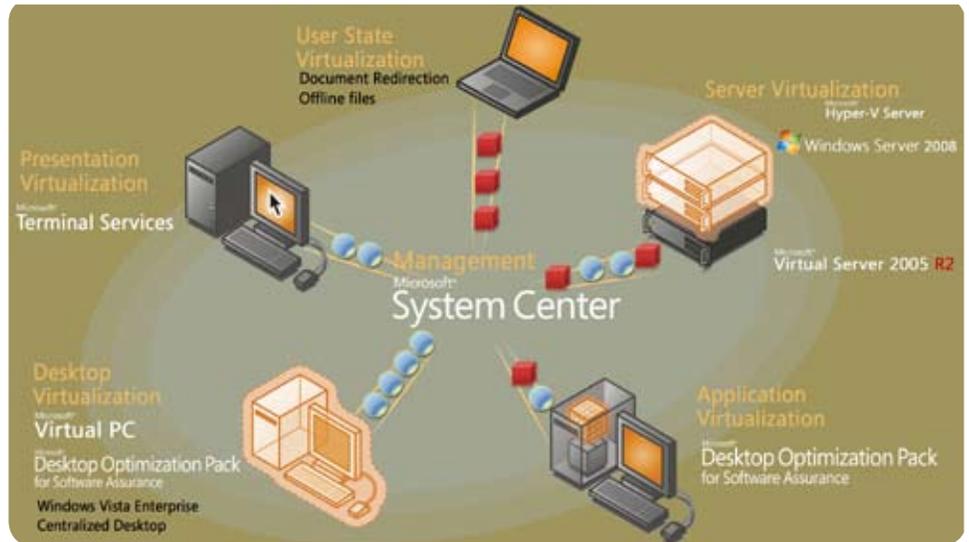
## Desktop Virtualization

*Choose how to virtualize the desktop for user flexibility and IT control*

In today's IT environment, it is a constant challenge to support the numerous applications found across an organization. Legacy applications and other software outside of the standard image require compatibility testing and additional time spent resolving application conflicts. Furthermore, in a traditional model, each PC is loaded with applications installed for the individual user, making migration planning a complex, labor intensive practice.

Virtualization is used to address these problems by decoupling user data, application functionality, and settings from the operating system and/or decoupling the operating system from the physical hardware. By delivering applications from a centrally managed server, application compatibility issues are minimized, ongoing maintenance is greatly simplified, and migration is faster and easier for both IT and end-users. By provisioning virtual desktops, adoption of new technologies is accelerated, desktop image management is simplified, and end-user flexibility and mobility are increased.

### Five Types of Virtualization



Virtualization is used in many facets of the IT infrastructure and can be applied to a wide range of components, whether the desktop, the server, an application, the presentation layer, or a user profile. With a far reaching impact, virtualization plays a key role in the optimization of the IT infrastructure.

#### Basic → Standardized

##### Virtualize Storage, Hardware or Application Issues

- Virtualize profile to store data and settings on servers
- Virtualize applications or exceptions to the standard image

##### Benefits

- Simplified data back-up and availability
- Removes barriers to a standardized image
- Application-to-application conflict solution
- Easier delivery of non-standard applications
- Simplified support for hardware exceptions

##### Implementation Guidance

- Windows Springboard Implementation Guide – “Improving system Resiliency, Reliability, and Hardware Performance” <http://technet.microsoft.com/windows>

#### Standardized → Rationalized

##### Virtualize to Maximize Efficiency

- Deliver virtualized applications on demand
- Use Virtualized Desktop Infrastructure to extend the life of hardware that won't meet requirements

##### Benefits

- Reduced costs for deployment and maintenance
- Lower software and hardware costs
- Faster and cheaper problem resolution through centralized administration
- Increased flexibility

##### Implementation Guidance

- Windows Springboard Implementation Guide – “Advanced desktop management approaches” <http://technet.microsoft.com/windows>
- Windows Springboard Implementation Guide – “Meet Emerging Compliance and Governance” <http://technet.microsoft.com/windows>
- Core IO – Secure remote access to internal resources and LOB applications beyond email <http://technet.microsoft.com/library/bb821287.aspx#EGAA>

**User State Virtualization** – Separate processing from user data and application settings, making it possible to run an application in one location but access files in another. This facilitates server-based data backup, allows users access to files from any PC, and makes it easy to migrate a user to a new computer or upgrade the operating system without losing data.

**Application Virtualization** – Separate the application configuration layer from the desktop OS to reduce application conflicts and bring patch and upgrade management to a central location that accelerates the deployment of new applications and updates.

**Desktop Virtualization** – Create a separate desktop OS environment to run applications that are not compatible with a new operating system, and to create multiple, separately managed desktop environments on a single PC. Desktop virtualization can be server-hosted (virtual desktop operates on a server and is remotely accessed by the user) or client-hosted (virtual desktop operates locally on the user's PC).

**Presentation Virtualization** – Separate the processing from the graphics and I/O, making it possible to run an application on the server while it is controlled from the desktop, as is done with Windows Terminal Services. This is helpful in a variety of situations, including ones where data confidentiality and protection are critical.

**Server Virtualization** – Separate the OS environment from the host server for optimal resource use with operational isolation and security. While this is not a form of desktop virtualization, this is useful for testing desktop applications for compatibility before deployment.

## Rationalized → Dynamic

### Information and Application Access Anywhere

- ☑ Deploy role-based configurations, one VM for multiple users, which are independent of hardware and OS
- ☑ Provide seamless migration for mobile computing, enabling personalized applications and computing environments anywhere
- ☑ Provide shared server-based computing for task workers with centrally stored data

#### Benefits

- Lower time and costs for configuration and troubleshooting
- Reduced end-user downtime when migrating across PCs and computing devices
- Greater end-user flexibility and mobility, with “go anywhere” computing

#### Implementation Guidance

- Windows Optimized Desktop Scenario – Videos <http://www.microsoft.com/windows/products/windowsvista/enterprise/scenarios.mspx>

## Key Benefits

Virtualization delivers significant benefits throughout the desktop infrastructure. A few key benefits include:

**Reduced Application Conflicts** – By handling software and hardware exceptions outside of the standard image, virtualization enables the delivery of applications without time- and cost-managing compatibility issues.

**Lower Cost for Deployment and Maintenance** – By enabling the delivery of applications from a central server, virtualization helps to dramatically streamline software deployment and ongoing patching and updates.

**Greater Computing Flexibility** – By virtualizing multiple computing layers, including the desktop, the application, and the profile, organizations are able to deliver personalized computing environments to their end-users anywhere and anytime they need it.

## BASF IT Services Company Streamlines Desktop Deployment with Software Virtualization

**BASF IT Services**

■ BASF Gruppe

### Situation

BASF IT Services supports nearly 60,000 users worldwide and needed a way to shorten application deployment time while still keeping certification at the same high level of quality.

With virtualized applications, there's nothing to distribute; the virtualized program is “streamed” to the PC and can be used without installing. The Microsoft SoftGrid client software, which needs to be distributed only once, works the same for each streamed program. For the administrator, application administration consists of nothing more than assigning a user to the correct Active Directory group.

Several thousand users are already using programs that have been virtualized with Microsoft SoftGrid, but they don't even notice. Programs are launched using the same icon or Start menu entry, just like they always have. Performance has not suffered from streaming.

### Results

*“Feedback from our customers is overwhelmingly positive—programs and updates are available sooner.”*

*“By implementing SoftGrid, we've simplified processes, and we need less detailed knowledge about the applications we're distributing. This allows us to respond to our customers' demands more quickly and efficiently.”*

**Frank Walburg**  
Department Manager of Desktop Software Services  
BASF IT Services

<http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000001313>

## Best Practice 4:

## MANAGE

## Automated Management

Manage automated software updates, central configuration, and policy, with remote monitoring and support

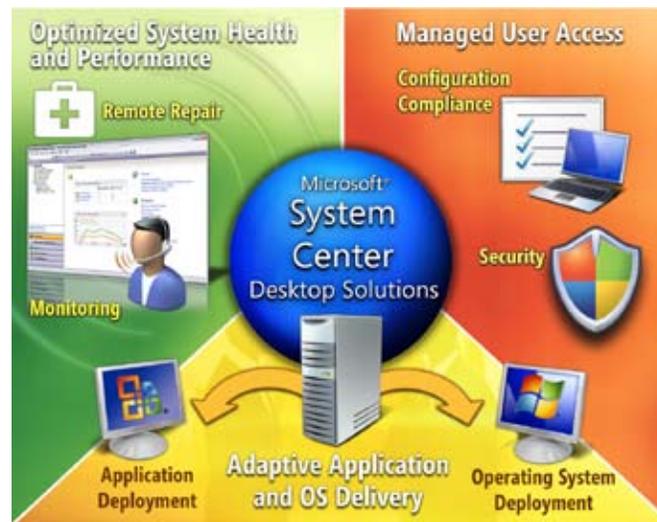
The IT department is continually challenged with managing complexity in the PC infrastructure—often overseeing diverse computing environments and applications, and ensuring that they are secure, up-to-date, and fully operational. To keep IT labor costs down, and to keep end-users productive, many IT departments are turning to a greater use of automation and more centralized configuration and policy setting. They are seeking the ability to remotely monitor and maintain the health of the organizations' PCs.

### Establish the Network Directory Service

To start streamlining IT management, the organization must first establish a network directory service and policies as a way of keeping track of the PCs on the network. A network directory service forms the foundation for organization-wide PC management. It is essential for authentication and authorization, and it also

enables administrators to assign policies, deploy software, and apply updates to an organization.

### Centralized PC Management



### Create Groups and Set Policies

Next, IT can organize PCs and other resources into groups, based on roles, hierarchies, geographies, and other relevant factors. Rights and policies are then assigned using these groups, forming the foundation for automating PC management tasks.

### Automate Software Updates

Once a network directory and group policies are established, IT can automate the deployment of patches and software updates. Moving to light touch and then zero touch patch and update deployment not only saves IT time, but also improves security by reducing the window of potential vulnerability between updates.

#### Basic → Standardized

### Network Directory Services and Group Policies

- Establish Active Directory® as the foundation for centralized PC management
- Create groups and assign Group Policies for improved control and automation
- Use agentless issue reporting to improve responsiveness for updates and troubleshooting

#### Benefits

- IT labor savings from centralized management and reduced PC support needs
- Increased system uptime with a managed desktop environment and faster problem resolution
- Strengthened security through faster patches and updates

#### Implementation Guidance

- Core IO – Unified Directory with Directory Aware Client <http://technet.microsoft.com/library/bb821256.aspx>
- Core IO – Administrator-controlled automated patch distribution for desktops <http://technet.microsoft.com/library/bb821257.aspx#EJAA>
- Windows Springboard Implementation Guide – “Group Policy Configuration Management to Reduce Help Desk Calls” <http://technet.microsoft.com/windows>

#### Standardized → Rationalized

### Automate and Monitor

- Perform targeted application deployment and patching, including security updates
- Use enterprise-wide application error monitoring, including proactive monitoring of critical PCs
- Provide remote help desk support using screen sharing remote PC assistance

#### Benefits

- Reduced IT labor costs for patching and deployment
- Proactive PC monitoring and faster updates and problem resolution
- Improved help desk responsiveness and efficiency

#### Implementation Guidance

- Core IO – Defined and enforced configuration standards on desktops <http://technet.microsoft.com/library/bb821283.aspx#EAAA>
- Core IO – Formalized application compatibility testing and packaging <http://technet.microsoft.com/library/bb821285.aspx#EFAA>
- Windows Springboard Implementation Guide – “Advanced desktop management approaches” <http://technet.microsoft.com/windows>

### Centralize Configuration and Policy

One of the most effective drivers of IT labor productivity is centralized management of PCs across the network. The gain in efficiency and control that centralized management of the desktop environment provides leads to greater stability, faster problem resolution, and fewer issues with software deployments and patches. Limiting end-users' ability to change settings and configurations can help to avoid potential application conflicts and reduce the downtime events often found in unmanaged IT environments.

### Enable Remote Monitoring and Support

Another key component to streamlining PC management is the use of effective tools for remote monitoring and support. Using real-time application monitoring, the IT staff is quickly alerted, and so can respond right away when updates are needed, or when problems arise in the desktop infrastructure. Critical PCs can also be flagged for proactive monitoring. IT can then use screen sharing for remote PC assistance to troubleshoot and resolve issues immediately. Ultimately, by enabling policy-based desktop control, remote monitoring and maintenance can be performed to increase up time and reduce the costs of IT support.

### Key Benefits

More effective IT management creates benefits throughout the organization, not only by helping to reduce IT-related costs but also by making a direct impact on the productivity of the information workers in the organization.

## Rationalized → Dynamic

### Full Automation with Remote Support

- ☑ Automate individual changes and routine processes to shift IT focus to exception handling and policy management
- ☑ Automatically propagate software changes enterprise-wide
- ☑ Create centralized desktop configuration database and monitor drift from compliant baseline configuration
- ☑ Enable enterprise-wide remote access, diagnosis, and repair

#### Benefits

- Dramatic reduction in manual IT tasks
- Automatic protection against control policy compliance drift and application compatibility issues
- Higher IT services levels with reduction in routine maintenance
- Improved prioritization of IT resources for increased business agility

#### Implementation Guidance

- Windows Springboard Implementation Guide – "Remote Management of Laptop PCs" <http://technet.microsoft.com/windows>
- Core IO - Model-enabled service level monitoring of desktops <http://technet.microsoft.com/library/bb821282.aspx#EDAA>

**Greater Control** – With a network directory service and Group Policies, IT has improved control over desktop configurations and maintenance, ensuring that systems are highly secure, up-to-date, and in compliance with established policies.

**IT Labor Savings** – Improving IT management cuts IT labor costs by dramatically streamlining the processes involved in update deployment, PC maintenance, and help desk support.

**Increased System Up Time** – With a more controlled desktop environment and faster problem resolution, end-users benefit from fewer disruptions and greater productivity in their jobs.

**Improved Security** – Automated patching and updates, combined with proactive application monitoring, helps IT reduce the window during which potential security vulnerabilities may exist.

## Fulton County Government Enhances IT Security and Manageability



### Situation

The government of Fulton County serves a population of nearly one million in northwest Georgia. Its IT department supports 5,000 employees in 400 buildings, dozens of agencies, airports, fire stations, police stations, courts, public-health clinics, and libraries.

Even with a desktop that was firewall enabled, the County needed greater protection, as evidenced by virus attacks in 2003 spread via county-owned mobile computers. Instead of the cumbersome, paper-based policy of the past, Fulton County is using Network Access Protection to enforce standards, policy, and system-health compliance. The County decided to deploy NAP to all clients on its IT infrastructure and deployed a Domain Isolation solution that put all clients into a single logical network domain. To support NAP, the County is deploying Windows Server 2008 on its servers, and the Windows Vista® or Windows® XP SP3 operating systems on desktop and notebook computers.

### Results

The county has been able to reassign two full-time maintenance staff members to new technology initiatives, resulting in IT maintenance cost avoidance of U.S. \$ 157,000 annually.

*"We anticipate that System Center Configuration Manager will help us implement NAP very smoothly."*

*"Using System Center Operations Manager 2007 reporting tools, we will know immediately whether a client is in compliance."*

*"We have reduced help-desk calls from an average of 20 per day for a user group of similar size down to just 5 per day—a 75 percent improvement."*

**Robert E. Taylor**  
CIO/Director of Information Technology, Fulton County

<http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=4000001286>

## Best Practice 5:

SECURE

## Comprehensive Security

*Provide integrated comprehensive security and data protection with improved compliance*

The frequency and sophistication of IT security threats is constantly on the rise, requiring an ever greater investment in time and resources by the IT department. The risks posed to organizations are varied and far-reaching—from the theft of IP and sensitive data to lost productivity as a result of debilitating malware attacks. Security remains high on the list of concerns for IT departments today. These trends underscore the need to provide robust desktop protection, and as a result, organizations are focusing their efforts on creating well-integrated and comprehensive initiatives for security and data protection in the desktop environment.

### Fundamental PC Self-Defense

The first step toward integrated security is to ensure that each PC has the rudimentary tools needed for its own defense. To limit access across a network and prevent unauthorized sharing, a personal firewall must be enabled on each PC. Anti-virus, anti-spyware, and anti-malware

software should be installed and configured to run and self-update automatically. PCs that contain confidential data require encryption to be fully protected. Finally, a solution is needed to report on attacks, configuration, and updates—and to support centralized security policy management.

### Comprehensive Security



### Integrated and Comprehensive Security

When numerous narrowly focused point solutions for security (such as individual anti-spyware and anti-virus programs) are used, they involve multiple management consoles and disjointed event reporting and analysis. This makes security management more complex—and potentially less effective. To create more comprehensive desktop security, organizations can unify solutions across a range of areas including malware prevention, data protection, and identity management. A comprehensive approach to security that incorporates single sign-on and federated trust between organizations offers businesses

improved security while providing end-users more seamless and better-controlled access to networks and data.

#### Basic → Standardized

##### PC Level Security Tools

- ☑ Ensure that all PCs on the network have the fundamental tools for self protection, including:
  - Personal firewall
  - Anti-spyware/malware protection
  - Disk-based data encryption
  - Basic security reporting

##### Benefits

- Prevention of unauthorized access to networked PCs
- Protection against the latest spyware, virus, and malware attacks
- Greater protection of data on lost or stolen laptops
- Reporting and alerts for proactive security maintenance and fast response when issues arise

##### Implementation Guidance

- Core IO - Auto-updating antivirus software on PCs <http://technet.microsoft.com/library/bb821258.aspx#EHAA>
- Windows Springboard Implementation Guide – “Security Hardening & Defense-in-depth” <http://technet.microsoft.com/windows>

#### Standardized → Rationalized

##### Unify Protection and Identity Management

- ☑ Enable single sign-on for more controlled and simplified end-user access
- ☑ Create federated trust between organizations
- ☑ Deploy enterprise malware monitoring and response
- ☑ Enable cross-enterprise data protection
- ☑ Deploy multi-factor authentication for high-risk scenarios

##### Benefits

- Well-integrated and more comprehensive data security and access control
- Faster maintenance and deployment of the latest security solutions and tools
- Stronger authentication and access protection

##### Implementation Guidance

- Springboard/Technet
- Core IO - Policy-managed local firewall on desktops <http://technet.microsoft.com/library/bb821287.aspx#EHAA>
- Core IO - IPSec or certificate services <http://technet.microsoft.com/library/bb821287.aspx#EBAA>
- Core IO - Secure wireless network using Active Directory <http://technet.microsoft.com/library/bb821287.aspx#ECAA>
- Windows Springboard Implementation Guide – “Security Hardening & Defense-in-depth” <http://technet.microsoft.com/windows>

### Strengthened Data Protection and Access Control

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. This includes ensuring that data is encrypted and that multi-factor authentication can be deployed for access in high-risk scenarios.

### End-Point Security with Content-Level Granularity

Organizations with an optimized infrastructure are able to use content-level granularity to provide end-point security that extends and enhances network-based security to groups and individuals. For example, controlling who can access or print a particular document or email — resulting in protection and follow the content. This provides multiple layers of security for increased protection.

### Real-Time Security Reporting and Monitoring

With desktop optimization organizations use real-time security reporting and monitoring to proactively and automatically defend against new threats, including threats not yet characterized or known to the enterprise. This means that potential issues can be discovered, contained, and solved early, before the impact is compounded and expanded throughout the organization.

### Expanding Security Beyond the Enterprise

In the Dynamic desktop environment, organizations can extend trust-based federation to Web services. Using these Web-based trust services and identity management, IT can bolster security both in the enterprise network and beyond.

## Rationalized → Dynamic

### Comprehensive, Fully Automated, Granular, Security and Compliance Support

- Enable Web-based trust services and identity management
- Deploy end-point security with content-level granularity
- Use real-time reporting and monitoring to defend against threats not yet known to the enterprise

#### Benefits

- Strengthened security within the enterprise network and beyond
- Extended and enhanced network-based security
- Faster threat response and improved prevention

#### Implementation Guidance

- Core IO - Integrated threat management and mitigation across client and edge <http://technet.microsoft.com/library/bb821282.aspx#EEAA>
- Windows Springboard Implementation Guide – “Security Hardening & Defense-in-depth” <http://technet.microsoft.com/windows>

### Key Benefits

By taking a comprehensive and well-integrated approach to security, organizations benefit from improved protection and access control, and the IT department is able to remain proactive in combating the latest threats.

**Comprehensive Protection** – By integrating solutions for a wide range of security and access needs, organizations can provide multi-layered protection across the entire PC infrastructure and beyond.

**Faster, More Efficient IT Security Management** – With integrated, real-time security alerts and reporting, IT can respond more quickly, and often work more proactively to prevent threats before they occur.

**Improved Access Control** – By combining identity management and content-level granularity, organizations have the tools for multiple level of access control, strengthening access protection and enabling end-users with anywhere access to the applications and data for which they have permissions.

## Brazilian Pipeline Operator Enhances IT Security with Software Upgrade



### Situation

Comgás is the largest distributor of piped natural gas in Brazil, with a pipeline network of approximately 3,100 miles that supplies gas to more than 550,000 residential, commercial, and industrial consumers.

Over three months, Windows Vista and the 2007 Office System were installed on more than 900 computers across several Comgás offices utilizing the Microsoft Solution Accelerator for Business Desktop Deployment (BDD) 2007 and Microsoft Application Compatibility Toolkit (ACT) 5.0. In addition, to further reinforce its IT security infrastructure, Comgás adopted Microsoft Forefront™ Client Security to help protect its workstations against viruses and spyware.

### Results

*“New security features in Windows Vista and Forefront Client Security software are helping Comgás to secure its IT environment and improve management efficiency. For instance, the company is taking advantage of the personal firewall, disk-encryption system, and antivirus capabilities that are integrated into Windows Vista. We used to use totally independent solutions to fight viruses and spyware, making environment management more complex. Now our environment is under greater control and protection due to the tools integrated in Windows Vista and Forefront. Additionally, it is much easier to identify possible security risks.”*

**Jaime Mesquita**  
IT Manager, Comgás

<http://www.microsoft.com/casestudies/casestudy.aspx?casestudyid=400001920>

## Conclusion

By examining these best practices and scenarios you now have an understanding of the tangible benefits and employee productivity gains that can be achieved through desktop optimization. In addition, this paper has mapped the concrete steps that you can take to help your organization realize those benefits.

The road to desktop optimization is a journey. The five best practices we have covered provide a way to achieve major benefits in the short-term, and they offer a long-term roadmap toward a more profound transformation in the way your organization operates. Capturing information about your organization and your IT processes, and then using that information to build an optimized infrastructure is at the heart of this transformation. IT maturity cannot be achieved by purchasing software alone. It is ultimately achieved by combining recognized best practices with software uniquely configured to each organization to form an infrastructure that unlocks the potential of your people.

By taking the path toward desktop optimization, you are preparing your organization for a future in which business agility is an imperative to remain competitive. The path to getting there is now clear. With these best practices and guidance, you are ready to build an infrastructure based on well-integrated solutions and technologies that are optimized to drive the success of your business.

## Take the Next Steps—Begin the Journey

- 1. Assess Your Current IT Environment** – Contact your Microsoft or your Partner account representative to get your Core IO assessment, or take the Core IO Self-Assessment at <http://www.microsoft.com/IO>.
- 2. Plan for Success** – Explore joint planning with Microsoft or your Partner account representative to identify projects, prioritize them by level of impact, and develop your PC lifecycle strategy.
- 3. Utilize Guidance and Resources** – Provide project implementation guides and other resources to your IT professionals so that they may review and assess areas of opportunity. (These are referenced in the IO step rate boxes on each of the best practice pages.)
- 4. Tap into Available Expertise** – Consult with the experts at Microsoft Services or your Microsoft Partner who are well-trained to help you optimize your infrastructure. These expert guides will work with your IT staff to take your PC strategy to the next level and realize the maximum benefits from your Microsoft technology.
- 5. Create a Proof-of-Concept** – To assist you on your journey to optimization, the experts at Microsoft Services or your Microsoft Partner can help you develop a Proof-of-Concept to demonstrate the value of IO progression in your organization.

## Additional Resources

### Products:

Windows Vista Enterprise [www.microsoft.com/windows/products/windowsvista/enterprise](http://www.microsoft.com/windows/products/windowsvista/enterprise)

Microsoft Desktop Optimization Pack for Software Assurance

[www.microsoft.com/windows/products/windowsvista/enterprise/benefits/tools.msp](http://www.microsoft.com/windows/products/windowsvista/enterprise/benefits/tools.msp)

Microsoft System Center [www.microsoft.com/systemcenter/en/us/dynamic-desktops.aspx](http://www.microsoft.com/systemcenter/en/us/dynamic-desktops.aspx)

Microsoft Forefront Client Security [www.microsoft.com/forefront/clientsecurity](http://www.microsoft.com/forefront/clientsecurity)

Microsoft Office 2007 Enterprise Edition <http://office.microsoft.com/en-us/suites/FX101674041033.aspx>

### Services:

Microsoft Services <http://www.microsoft.com/services>

### Resources:

Core Infrastructure Optimization [www.microsoft.com/IO](http://www.microsoft.com/IO)

Solution Accelerators <http://technet.microsoft.com/solutionaccelerators/>

Alinean ROI Tool <https://roianalyst.alinean.com/microsoft/iotool/launch.html>

Springboard Series Resources for IT Pros <http://technet.microsoft.com/en-us/windows/aa904820.aspx>

## Microsoft's Desktop Optimization Solutions

Microsoft offers a complete solution of integrated products and services for optimizing the desktop infrastructure. Together, these solutions deliver organizations a range of powerful capabilities that simplify desktop deployment and management, improve security and compliance, and provide access to applications and data from anywhere. Many of these products and technologies are already in use in your organization. As you progress through the Core IO levels, you will be able to extend your technology investment by unlocking its full potential – using advanced capabilities of software and resources that you already have in place.

# Microsoft Desktop Optimization - a Well Integrated Solution

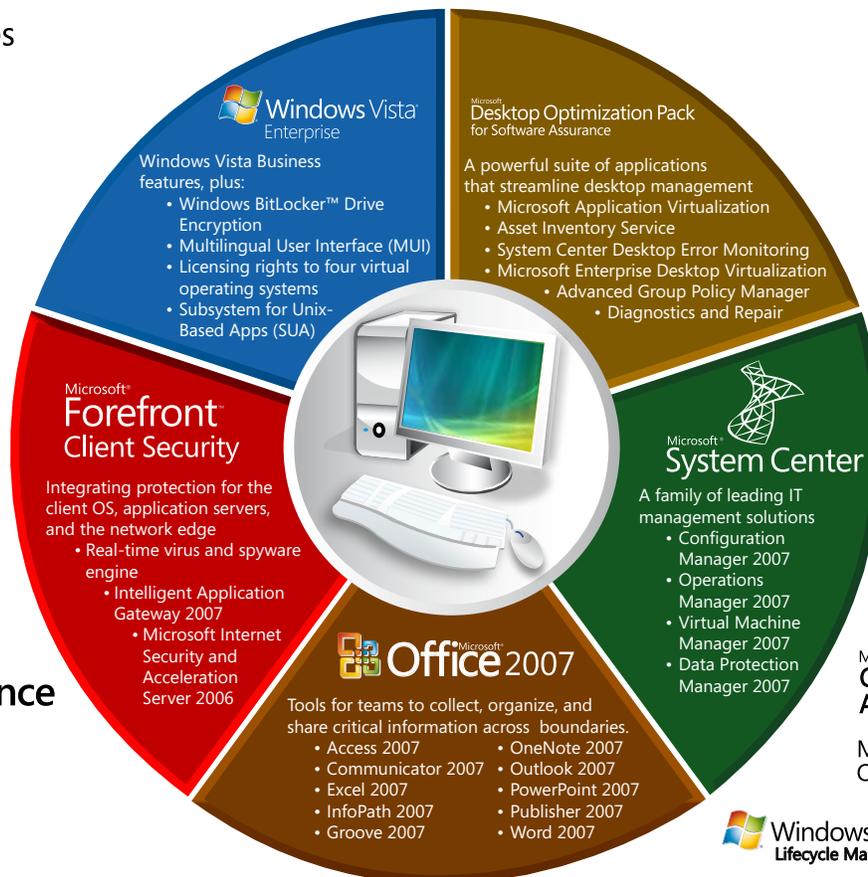
## Microsoft and Partner Services

### Microsoft | Services

- Desktop Optimization Services using Microsoft Windows Vista and 2007® Office System® (DOVO)
- Desktop Deployment Planning Services (DDPS)
- Design and Implementation for Active Directory (DIAD)
- Configuration COM Manager Optimization
- Service Manager Optimization (SMO)
- Security, Identity and Access Management (SIAM)
- Application Compatibility Factory (App. compat.)

Microsoft  
**Software Assurance**  
for Volume Licensing

## Product Portfolio



## Implementation Resources

**SOLUTION ACCELERATORS**  
Act faster. Go further.

- Microsoft Assessment and Planning
- Microsoft Deployment Toolkit
- Infrastructure Planning and Design Guides
  - System Center Operations Manager
  - System Center Virtual Machine Manager
  - Microsoft Application Virtualization
  - Terminal Services
- Security Guides
  - Windows Vista
  - Office 2007

**Springboard Series**  
Implementation Guides

Microsoft®  
**Core Infrastructure Optimization Assessment**

Microsoft  
**Operations Framework**  
Proven Practices for Operational Excellence

Windows Vista Lifecycle Management | Alinean ROI Tools | PC Lifecycle Whitepaper

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

©2008 Microsoft Corporation. All rights reserved.

Microsoft, Access, Active Directory, BitLocker, Excel, Forefront, Groove, Hyper-V, Internet Explorer, Office, Office logo, Outlook, PowerPoint, Security Shield logo, Visio, Windows, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.