

A Best Practice Approach to Implementing a Proactive Patch Management Strategy

AUGUST 2007

Raymond Cadden

BUSINESS SERVICE OPTIMIZATION

Table of Contents

Executive Summary

SECTION 1 2

The Need to be Proactive

The One Constant — Available Patches

The Patch Management Landscape — An Overview

The Patch Management Challenge

The Patch Management Process

The Difficulties Faced by Each Enterprise
Are Different

SECTION 2 6

Planning Best Practices

Planning the Implementation

Establish Patch Management Service Level
Agreements

How Will the Patch Management Lifecycle be
Managed?

Architectural Concerns to Support the Strategy

Choosing the Appropriate Patch to Deploy

Change Management Integration

What Reports Are Required?

Communicating the Strategy to the User Community

SECTION 3 11

Implementation and Operational Best Practices

Communication

Pilot Deployment

Enterprise-wide Deployment

Continue to Monitor

Patch Maintenance

Change Management

Patch Management Strategy Review

SECTION 4 12

Conclusions

SECTION 5 12

About the Author

ABOUT CA Back Cover

Executive Summary

Challenge

Today's enterprise relies upon a successful patch management strategy to ensure the availability of end systems and maintain business continuity. Affecting every area of the IT infrastructure, effective patch management is a combination of people, technology and best practices.

However, ongoing patch management is one of the biggest challenges within IT departments today. In an effort to address the need, there is a rush to implement technology in isolation, often with minimal planning, and without a comprehensive ongoing operational plan.

As the enterprise becomes more complex and the wave of patches continues to increase, introducing changes on the fly is no longer an option. Without a cohesive best practice approach, proactive patch management is an elusive goal.

Opportunity

Unmanaged change is one of the most common causes of disruption to the IT infrastructure, and subsequently, the business. Each patch deployment is considered a change to the environment, and therefore needs to be proactively managed in order to ensure continuity of business functions.

A comprehensive patch management strategy requires the successful and seamless execution of disparate functions. The strategy should employ best practices and address patch planning through implementation, as well as ongoing operations in order to ease the impact of change. Without a comprehensive strategy from the onset, the enterprise may need to treat each new patch as a brand new initiative, making it necessary to continually react and adapt in order to support the business with each patch deployment.

Benefits

Introducing change on the fly is no longer a suitable approach to patch management.

A best practice approach to implementing a patch management strategy provides the necessary uniform process framework to manage the patch lifecycle in a timely, controlled and uniform manner. This approach enables organizations to meet the required service levels needed to support the business, while:

- Increasing availability of end systems
- Ensuring business continuity

SECTION 1

The Need to be Proactive

The One Constant — Available Patches

In an ever-changing IT world, there is one constant — the number of available software patches continues to increase. As the enterprise moves to support new business initiatives, additional software is introduced to the environment. The permutation of software, platform, configuration and ownership (both IT and business) increases the complexity of the IT environment, making the task of keeping each software component at its most current patch level, all the more difficult.

The difficulty in coordinating and managing these changes can often result in end systems receiving a required patch more than six months after that patch is made available.

A best practice approach to defining a patch management strategy; combined with people, technology and operational best practices; allows the enterprise to move from reactive patch management to proactive patch management, significantly improving availability and business continuity, while achieving economies of effort.

The Patch Management Landscape — An Overview

To understand the need for best practices, both in defining a patch management strategy and providing ongoing patch management operations, it is important to gain some perspective on the patch management landscape from the available historic overview.

According to the CA Content Update Service¹, in the twelve month period ending August 2007, Microsoft has released 68 bulletins, (44 were defined as CRITICAL), containing 379 software patches. In the previous twelve month period, ending August 2006, there were 63 bulletins (38 defined as CRITICAL), containing 383 software patches.

Given the constant wave of software patches from all software vendors, it is clear that the need to perform patch management will continue, and organizations need to develop a unified patch management strategy in order to adopt a proactive patch management posture. Making this transition will always be an ongoing and continuous effort, perhaps an unobtainable goal, without the adoption of patch management best practices.

¹ CA Content Research Team — <http://www.ca.com/upm>

The Patch Management Challenge

The patch management challenge is compounded by several factors:

- **Volume** New patches are released on a daily basis. Necessary and required patches for the enterprise must be identified and evaluated as they are released.
- **Complexity** Each patch must be validated and researched to determine the patch signature, pre/post-requisites and dependency metadata. Patches may be complex, and may require domain expertise to deploy correctly.
- **Speed** Time is increasingly becoming a crucial factor. To be effective, patches often need to be deployed rapidly. A delay in their deployment may have a significant impact on the business.
- **Impact** Each patch is a change and requires formal testing before being deployed. Patches may cause other items to break or perform differently.
- **Event Driven** Patch management is often a reactive effort, performed only after the business is impacted.
- **Environment Change** New client devices are introduced to the enterprise on a daily basis. These assets need to be automatically discovered and patched to the desired patch level.

The ability to properly manage the process directly affects the integrity of the enterprise systems, their availability, and consequently the business itself. Manual or ad-hoc approaches, often driven by a media announcement of an available critical patch, are ineffective and may take days or weeks to deploy.

The Patch Management Process

Day-to-day, the patch management process is cyclic and complex, requiring the successful and seamless execution of disparate functions to operate correctly and effectively (See Figure Below).

THE PATCH MANAGEMENT LIFECYCLE



Awareness of newly available patches is the first step in the process, and needs to be monitored on an 'on-going' and real-time basis, as all patches are not released per a defined schedule.

Each enterprise is unique and not all patches may be applicable to every enterprise. Each enterprise must identify which patches are relevant to their environment. This is a critical phase of the patch management process, and one in which reactive manual approaches inevitably fall short.

Newly applicable patches must then be validated to insure that they are what they advertise them to be, and researched to determine unique dependencies, pre- and post-requisites. This phase of the process is complex, time-consuming and traditionally error-prone.

Once validated, the patch enters the testing phase of the patch management process. Patches that pass the testing phase criteria are approved and scheduled for deployment to the enterprise.

After approval, the next phase in the patch management lifecycle is the determination of specific systems that need patches. At a minimum, this complex task requires:

- An accurate up-to-date inventory of the enterprise assets
- The ability to determine the applicability of each patch to the individual asset
- The ability to ensure that the required pre- and post-requisite conditions are satisfied

The ability to quickly determine the status of every phase of the patch management process is critical. Accurate and meaningful reporting provides the enterprise with necessary insight into the patch management process and a current perspective of the enterprise patch management posture.

The deployment of necessary patches needs to be controlled and coordinated across the enterprise without impacting the business.

The final and ongoing phase in the process is assurance; the knowledge that previously deployed patches remain deployed within the environment and the desired state is maintained. To achieve this assurance, continuous monitoring of the enterprise assets for patch level compliance and reporting on non-compliance, or automatic re-deployment per defined policy, is required.

The Difficulties Faced by Each Enterprise Are Different

Though the patch management lifecycle implemented by each enterprise will align with the industry approach as outlined previously, each enterprise should best determine how to align their unique patch management approach with the business as well. Most often the difficulties inherent with defining a patch management strategy fall into the following areas:

LACK OF STANDARDS Enterprise standards exist in most facets of the business, and are equally important within the confines of a patch management strategy. Without standards, patch management approaches are often ad-hoc, and prone to varying interpretation at each stage of the process. A lack of standards impacts effective patch management and directly impacts availability and business continuity. It also increases the effort required to manage the patch lifecycle, as each patch deployment is treated as a new effort that must be managed differently than the last, instead of as a uniform patch deployment process where everyone knows their role and responsibility. Examples include:

- What is the required patch level for each software component?
- What are the officially supported operating systems and applications?
- Is there a defined patch level for new machines?
- Are there different patch level requirements for machines that perform a specific role?

EACH ENTERPRISE IS UNIQUE Each enterprise has a different expectation with respect to availability and business continuity, and therefore there is not one approach to patch management that will satisfy every enterprise. Indeed the existing combination of people, process and technology used to currently support the enterprise will also be charged with implementing a specific patch management strategy to best support the unique business goals. While it is important that each enterprise have patch management best practices in place, these best practices must be aligned with the business goals in mind. Some examples include:

- When must patches be deployed after becoming available?
- How are patches tested and approved for deployment?
- How are patches approved for deployment?
- What approvals are required to advance a patch through the lifecycle?

CHANGE MANAGEMENT Patch management by its very nature, introduces change to the IT infrastructure and needs to be managed accordingly. Most enterprises today have already instituted a change management process with respect to their client management functions.

Unfortunately, these established change management processes can be somewhat manual in nature, and primarily focused on the IT operational aspects of a change management process. The larger change management process is often the bottleneck in any patch management process, requiring the cooperation of many functional teams within the enterprise, including security management, application development, business owners and IT operations. In many enterprises, these communities remain distinct with fragile lines of communication, and despite assurances, escalations to the highest levels are often required to advance tasks through the change management process. Unless these communities work together, it will be impossible to execute an effective patch management process.

That being said, clearly defined best practices can make change management a smoother process, and should include the business owners, so that the process is directly aligned with the business needs.

Best practices enable the enterprise to harness automation within the patch management process with a uniform process to advance a patch through the lifecycle, ultimately reducing time to deployment, while improving availability and reducing risk to the business.

Planning Best Practices

Planning the Implementation

All too often, the enterprise patch management strategy is driven by the desire to use technology to address the short term need of deploying software patches. As the short term need is satisfied, incremental needs are continually identified by both the operational and business owners. Some of these incremental needs will include:

- The need for coordination between the business owners and the various IT departments prior to deployment
- Determining who is best positioned to make decisions that will advance each patch through the lifecycle
- Ongoing clarification of relevant patches that are important to the business
- Updated service level requirements

As each new need is identified, or makes itself known through an impact to the business, the patch management process becomes a constantly evolving strategy, making it difficult for the enterprise to adopt a proactive patch management posture. The need for constant modification of a patch management strategy can be reduced by taking the time to pause, define and implement patch management best practices to address the business service level requirements. Patch management best practices enable the enterprise to harness automation to better address the needs of the business. Without best practices, each new patch may be viewed as a new enterprise-wide initiative.

Establish Patch Management Service Level Agreements

Before defining your patch management best practices, a complete understanding of the expectations from the business needs to be defined. Without understanding the business service levels expected from a patch management strategy, it is impossible to determine the best approach for the enterprise. Just as each enterprise is unique from an IT perspective, the same is true for the service level requirements from the business. Service level discussions should include the following topics:

- What is the expected time period from availability of a new patch to deployment on an end system?
- Should there be different deployment time periods for:
 - Different end system groups?
 - Different business units?
 - Machines performing different roles, e.g. desktop, server?
 - End systems in different countries?
 - Patches of different criticality?
- Is there a need to prioritize patch deployment by software type or business application?
- Defining the internal IT service levels required to support the business service levels
 - Time to accept and test each patch
 - Time to approve and deploy each patch
- Who within the enterprise is required to participate within these discussions?

- Do we need an emergency deployment protocol for “deploy now” patches?
- How do we measure the established service levels?
- What is the process to be followed when service levels are not adhered to?
- How will we best communicate the service levels to the larger user community?
- Do the existing client management service levels need to be considered?

By defining the patch management service levels, we are by default, building the foundations of patch management best practices, as all the necessary personnel are required to communicate and provide their respective input to define the service levels.

A final note on defining these service levels: it is critical to ensure that the service levels are reasonable. Unreasonable service levels ensure an ongoing uphill battle to satisfy the business needs. If a service level is unreasonable, reset the expectation early on in the process.

Throughout the process, service levels should be communicated regularly to the interested parties and agreed upon. Communicating the established service levels to the larger user community ensures that everyone knows what to expect.

A SAMPLE SERVICE LEVEL Operating system patches:

- Test environment: Desktop / Laptop Images, Security Team Workstations
- Test to approval: 48 hours from publication
- Build patch policy (Pending Change Management review): 72 hours from publication
- Change Management Approval: 96 hours from publication

Application software patches

- Test environment: DC Tier 1 & 2 application test servers. DMZ Test nodes
- Test to approval: DMZ Test - 24 hours, Tier 1 & 2 - 72 hours
- Build and Schedule Deployment:
 - DMZ - 48 hours (Pending Emergency Change)
 - Tier 1 & 2 - 96 hours
- Change Management Approval:
 - Emergency DMZ - 48 hours
 - Tier 1 & 2 - 120 hours

How Will the Patch Management Lifecycle be Managed?

After defining patch management service levels expected by the business, the enterprise should determine how the process will be managed before rushing towards implementing a technological solution. Defining how the patch lifecycle will be managed, by whom, and the necessary actions to support those requirements is critical in ensuring that the technology supports the documented patch management service levels.

- Document administration roles and responsibilities for the management of the patch lifecycle for:
 - Each technology
 - Different business units

- Different locations
- Is delegation required? What is the approval process, and how are they maintained?
- Do the responsibilities need to be aligned with those within the enterprise client management strategy?
- What is the process to add new technologies to the supported technology list?
- Who are the change management owners and how will production maintenance windows be established and maintained?
- Who is responsible for documenting patch deployment policies and their maintenance?

Architectural Concerns to Support the Strategy

When patch management service levels, roles and responsibilities have all been defined, supporting architectural approaches can then be determined and aligned to support the management strategy. At a minimum, the following should be considered:

TOPOLOGY CONSIDERATIONS Will the patch management process be managed from a single point, or will delegation and/or autonomy be required?

- Enterprise Topology
 - Minimized administration costs
 - Centralized change management integration
- Domain Level Topology
 - Granular administration rights
 - May be best fit for datacenter implementations or regional requirements

NETWORK CONSIDERATIONS How will the patch management solution impact the network? Are there modifications to the existing network environment that will be required to implement?

- **Content Import** The solution will have to obtain the software patches for processing within the patch lifecycle. Placement of the patch management solution and assurance that it can obtain the appropriate software patches needs to be addressed. Does the enterprise network team need to make adjustments to facilitate the download via:
 - Standard FTP, HTTP, HTTPS?
 - Web proxy with authentication supported?
 - Or should an offline patch import approach be considered?
- **Bandwidth Constraints** The enterprise network needs to be able to support the additional bandwidth requirements to ensure that software patches can be deployed to all the necessary end systems in order to support the defined service level deployment window. This will require:
 - Identification of the best placement of the solution components
 - Evaluation of network links to ensure the necessary bandwidth
 - Determining an alternative approach to service those end systems that do not have access to the required bandwidth e.g. remote users, slow link connections

STORAGE CONSIDERATIONS Software patches are often large and need to be available for long periods of time, resulting in large repositories of software patches. Storage requirements for the necessary patches need to be considered when defining the supporting IT infrastructure.

- Consider number of languages per patch required within the environment
- Consider historic monthly releases as a gauge for future releases
- Calculate disk requirements for each component of your patch management solution
- Consider the disk space required on end systems

TARGET GROUP CONSIDERATIONS In order to ensure that the correct end systems receive the necessary patches, groupings of machines for eventual patch deployment need to be determined. Referring to the previously defined service levels, we now have the target grouping requirements to be satisfied in order to support business service levels. This may be by business group, department, application, system role type or indeed all computers to provide for an emergency enterprise-wide deployment.

The creation of enterprise-wide target groups may be a manual process or the ability to create dynamic target groups based upon attributes may be necessary. Whichever method chosen, the identification of the requirement is critical to the success of your patch management strategy.

Choosing the Appropriate Patch to Deploy

As patches are released on a continual basis, the enterprise needs to determine the best uniform approach for their environment to ensure that relevant patches are deployed.

- **Individual Patches** Each patch is deployed as it is made available from the software vendor, and moves through the patch lifecycle independent of all other patches. This increases the workload on both the patch administrator and on the enterprise, as coordination effort is required for each patch.
- **Roll-Up Patches** All patches for a specific period are packaged into a single patch package and advanced through the patch lifecycle as a single patch. This reduces the workload for both the patch administrator and the enterprise. The impact to the business is also reduced as a single reboot can be executed after the last patch in the package is deployed on each end system.
- **Service Packs** Rather than deploy patches on an ongoing basis, the enterprise may choose to install service pack releases. While this approach further reduces the workload, it does increase the risk to the business between service pack releases.

While the decision on which patch to deploy is unique to each enterprise, and may also be further unique to business units within each enterprise, the decision can now be aligned with the expectations from the business.

Change Management Integration

A patch management strategy is a combination of people, process and technology. To be effective, the patch management process should be integrated with the established change management processes within the enterprise, and is often based upon the client change management process.

While change management integration points will be unique for each enterprise, there are common items to be addressed by all enterprises:

- What is the best approach for integration?
 - Electronic integration via email or a service desk solution for collaboration and approvals
 - Manual integration via scheduled meetings of the required groups with verbal approvals
 - Some combination of both
- Definition of granular standard change order templates outlining the required documentation and approvals at granular levels
- The establishment of routine scheduled meetings with change management administrators to review the integration strategy on an ongoing basis

What Reports are Required?

Making the necessary and relevant reports available to the parties involved in the patch management process is a critical part of a patch management strategy. Without relevant reports, it is difficult, if not impossible to measure the performance of the process, and it also reduces the ability to make necessary adjustments to the process as a whole.

At a minimum, reporting should be able to measure our ability to support the required service levels of the business, and provide operational information to the patch management administrators who manage the solution.

While out-of-the-box reporting within patch management solutions may provide some of the required reports, the ability to create custom reports that will provide the relevant perspective to the different reporting consumers, IT, business owner, and compliance, should be investigated prior to implementation.

To further reduce the ongoing reporting burden on the patch management administrators, it may be preferable to devise automated delivery of the reports to the various change management team and IT groups.

Communicating the Strategy to the User Community

By its nature, a patch management strategy affects all end systems within the environment, and therefore needs to be communicated to all users within that environment. For example, when a patch is deployed to an end system, it is important that the user community is educated and;

- Is able to distinguish between an official enterprise patch deployment on their system, and a malicious software installation attempt. In the age of media alerts on malicious software, we want to ensure that the user does not attempt to circumvent the enterprise patch strategy by turning off their machines when a patch is being deployed for fear it is something that will impact their system.
- Can reduce the impact of a patch deployment on their system by understanding how to potentially postpone an installation or reboot to a time agreeable by them.

Implementation and Operational Best Practices

After employing a best practice approach for planning, it is equally important to follow a best practice approach for the implementation. An ad-hoc approach to the implementation will not only impact support of business objectives, but may also cause the perception that the approach is flawed, causing more effort on behalf of the project's proponents to address these unnecessary concerns. A best practice approach should contain the following steps:

COMMUNICATION Prior to the implementation, the goals of the implementation and the timelines should be communicated to the stakeholders so that they understand the process and the correct expectations are established.

PILOT DEPLOYMENT Choose a subset of enterprise end systems that are reflective of the whole enterprise environment (desktops, production application servers, remote systems), and manage the patch lifecycle for these systems with the patch management solution. Ensure that the agreed upon change management process is employed during this pilot phase. The length of the pilot phase should allow for sufficient testing and should be signed off by all proponents when it can be demonstrated to support the defined service levels. During this phase, it is imperative to review installation behaviors (How long does a deployment take? How long does a reboot of each system type take?), and test the available patch installation options.

ENTERPRISE-WIDE DEPLOYMENT Once the pilot phase has been successfully completed, begin the enterprise-wide deployment per a defined roll-out plan, making sure that enterprise users are aware of the rollout and have received education on how it will impact them, as well as the controls they have over the process.

CONTINUE TO MONITOR As the deployment is in process, continue to monitor the deployment, and all operational aspects to ensure that the deployment does not impact the business. The defined operational reporting will be critical on an ongoing basis.

PATCH MAINTENANCE As patches are accumulated over time, adherence to patch library pruning policies ensure that only required patches are stored, while others are archived should they be necessary at a later time.

CHANGE MANAGEMENT Regular reviews of the change are required to ensure that the necessary change management events are applicable and aligned with the business, and that the correct personnel are responsible for advancing patches through the lifecycle.

PATCH MANAGEMENT STRATEGY REVIEW The needs of the business will change as the business continues to change. Ongoing and regular reviews of the patch management strategy and associated service levels are critical to determine if those service levels need to be adjusted or integration with the change management process needs modification, in order to support the changing business needs.

SECTION 4

Conclusion

Each month, enterprise patch administrators are tasked with managing the patch lifecycle for newly available software patches. Without patch management best practices, this monthly task is often approached in a different manner each time, as the combination of newly available patches affects different areas of the IT infrastructure and the business, while consequently requiring unique coordination with the respective IT and business process owners. While this may be an acceptable approach to patch management for some, it cannot be considered a long term approach that will effectively support business needs, as manual, ad-hoc processes are time-consuming and prone to errors that impact the business.

A successful patch management strategy requires planning, implementation and operational best practices. A best practice approach to the planning phase ensures that the service levels required by the business can be defined correctly. These service levels drive the architecture and operational requirements of the patch management strategy concisely and the decision making process in choosing a technical solution.

Implementation best practices ensure that the patch management solution does not impact the business and is capable of supporting the business goals. Operational best practices allow each monthly software patch cycle to be uniformly managed and coordinated across the enterprise change management groups to support the business needs.

An ah-hoc approach to patch management is not practical in today's enterprise. Introducing change on the fly is no longer acceptable. A best practice approach to patch management is required to support the business and reduce the repetitive monthly IT effort.

SECTION 5

About the Author

Raymond Cadden, Product Manager, Unicenter Patch Management.

CA, one of the world's largest information technology (IT) management software companies, unifies and simplifies complex IT management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

WP05PCHMGT01E MP319150807