Data Sheet

Unicenter® Patch Management r11

Unicenter® Patch Management r11 offers a comprehensive solution that provides the automation and necessary process framework to address the complex desktop patch management challenges faced by companies of all sizes today. This scalable and secure solution ensures business continuity by proactively managing the software patch lifecycle, and provides a patch management process framework to enable enterprise desktop assets to operate effectively.

Key Features

- 24x7 Patch Research Content Team
- Desired Patch state Compliance and Assurance
- Patch Level Policy Templates

Requires

- Unicenter® Asset Management r11 and Unicenter® Software Delivery r11

OR

- CA Desktop Management Suite™ r11

Supported Environments

- Windows XP
- Windows 2000
- Windows 2003

The Patch Management Problem

Ongoing desktop patch management is one of the biggest challenges within IT departments today. Affecting every area of the IT infrastructure, patch management requires a dedicated, automated and managed solution.

The 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 desktops 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.

Today's enterprise depends on a successful patch management strategy to ensure availability and business continuity.

A proactive patch management approach begins with implementing a comprehensive patch management solution that employs the necessary automation to speed the patching process.

Comprehensive Patch Management

Unicenter Patch Management helps ensure business continuity by ensuring that enterprise systems are equipped with the most current software patches available, and provides the assurance that deployed patches stay in place and effective.

Unicenter Patch Management allows the administrator to manage the lifecycle of each patch, from monitoring and discovery of available patches, through patch research, patch packaging, package testing and their eventual deployment, and provides the necessary framework to manage the process effectively.

The result is a patch management process that is both structured and streamlined, reducing both the IT effort required, and the complexity.

Unicenter Patch Management builds upon the proven management foundations of Unicenter® Asset Management, Unicenter® Software Delivery and the CA Desktop Management Suite™.

The Patch Management Process

The patch management process is cyclic and complex, requiring the successful and seamless execution of disparate functions to operate correctly and effectively. Unicenter Patch Management simplifies this process (See Figure 1).

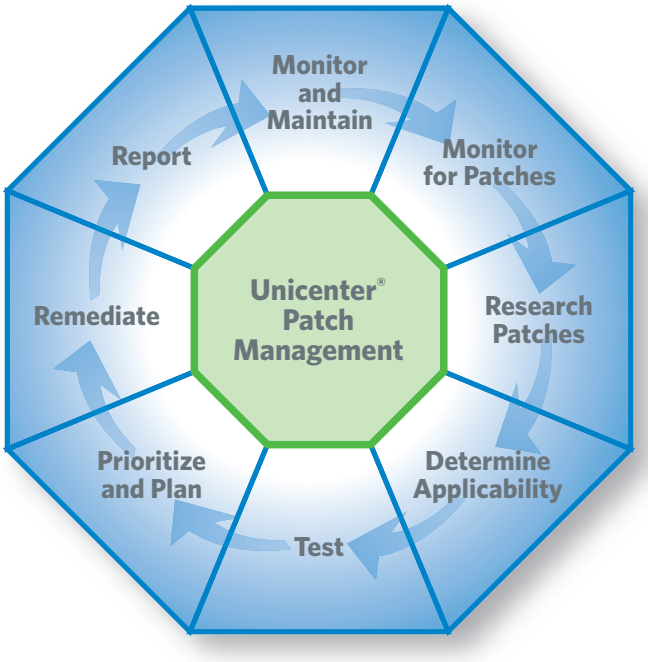

Figure 1.The Unicenter Patch Management Process.

Awareness of newly available patches and their applicability to the environment are the first steps in the process. This information needs to be monitored on an "ongoing" and real-time basis as patches are not released on a scheduled basis.

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, where 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.

The next phase in the patch management process is determining which systems need which patches. At 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 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.

Distinctive Features and Functionalities

Online Patch Management Content Research Team and Information Service. Staying aware of available patches, their relevance, impact, validation and dependencies is complex and time consuming. (See Figure 2) IT departments must be allowed to focus their efforts on decision making within the patch management process.

To alleviate burden on IT departments, Unicenter Patch Management is backed up by an online patch management content research team which performs the following functions:

- **Monitor.** Constantly monitors for newly available patches. Works proactively with major software vendors to know in advance what new patches will become available and when.
- **Validation.** Validates available patches, ensuring that they will install as described.
- **Research.** Performing the necessary patch research (determine patch applicability, patch signature, patch pre/post-requisites and dependency metadata).
- **Publish.** Publishes the enhanced patch metadata content on the Online Patch Information Service.
- **Make Available.** Automatically makes the enhanced patch metadata available to the enterprise. (See Figure 2)

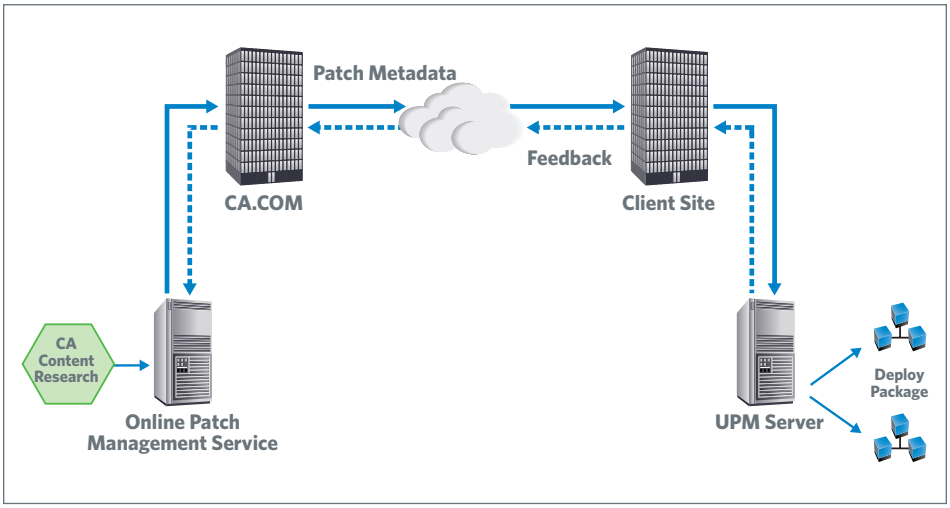

Figure 2. Solution Architecture.

- **Automated Determination of Systems Requiring Patches.** The ability to quickly determine which assets within your environment need, and are able to accept a newly available patch is a fundamental requirement for a successful patch management solution. Unicenter Patch Management automatically determines the systems that should receive the patch.
- **Detailed Knowledge.** Accurate knowledge of the IT assets, combined with the enhanced patch metadata provides the administrator with the information to decide which patches will be deployed to which systems.
- **Automated Analysis.** Advanced logic and detection mechanisms determine which patches are applicable to which individual enterprise resources.

Patch Testing. The Unicenter Patch Management solution facilitates and enforces a formal patch testing phase.

Packages (patch and metadata) are assessed against the required system configurations; impact is accessed and analyzed before the package is approved for enterprise deployment.

Patch Level Policy. Different assets within the enterprise will require different minimum patch levels based on their function, location, installed applications, and any performance requirements. The definition and maintenance of required patch levels for each class of asset is accommodated via:

- **Patch Policy Template.** The patch policy defines the patch level requirements of each asset class. Policies are updated as new patches become available.
- **Patch Policy Grouping.** Once defined, patch policies can be assigned per user defined machine group and applied manually, or as per policy.

Package Management. Patches must be packaged for deployment. Unicenter Patch Management simplifies this complex and time consuming task.

- **Automatic Package Creation.** Packages are automatically created by the Unicenter Patch Management server using the relevant patch metadata and then automatically registered for deployment.

Package Deployment. New patches are released at such a rapid pace that frequent deployment of packages is needed to keep enterprise assets current, productive and secure. Proactive patch distribution through automation is vital to controlling costs and ensuring availability and business continuity.

- **Automatically Initiated Per Policy.** Newly available patches are added to the patch policies, automatically initiating package deployments per defined policy. Using a policy based approach and a set-it and forget-it standard, Unicenter Patch Management eliminates the need for scheduling.
- **Patch Distribution Management.** Control, direct and manage all patch distribution actions from one central GUI.
- **Intelligent Patch Installation.** Provides the logic to help ensure that pre-, and post-requisites, dependencies and roll-up structures are applied for patch installations.

Administrator Control. A package deployment can be scheduled for a single system, a group of systems or the whole enterprise. Administrators can view reports on what patches are installed, where and when they were installed and who installed them. They can also see instantly the status of all active or scheduled deployments.

- **Reliable Delivery.** Built-in work flows and error controls keep track of what has been delivered and where it was delivered. Automated retries and extensive error reporting are available. A built in calendar allows patches to be scheduled to prevent conflicts and blackout periods can be defined for selected groups or systems.
- **User Access Control During Patch Installation.** The administrator can arrange for any logged in user to be forced to logoff or cause the deployment to wait until the user logs off on their own. Login is blocked until the job is complete.

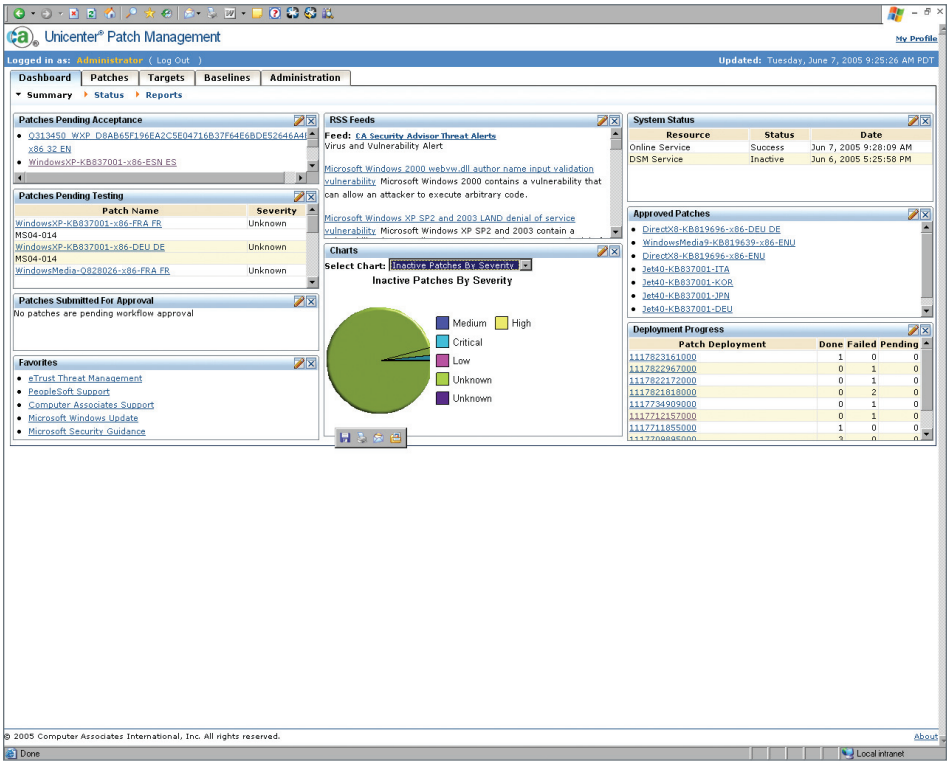

Figure 3. Each user can configure and populate their personal dashboard with the information they require.

- **Deployment Tracking.** Progress tracking of successful installations, scheduled installations, in-progress and failed installations.
- **Patch Roll Back.** Support for roll back of enabled patches.
- **Multiplatform Support.** Support for most major operating platforms is available.

Desired State Assurance. It is imperative that deployed patches remain in effect after deployment. The possibility exists for patches to be uninstalled or modified through subsequent user action. The enterprise needs to be able to automatically maintain, and verify the patch level desired-state of systems. Unicenter Patch Management offers patch level desired state assurance through:

- **Deployment Verification.** Continuous monitoring to ensure that applied patches/packages have not been compromised and are still valid and in effect.
- **New System Assurance.** Automatic restoration of a new or crashed system to the required patch level policy. This can also be combined with BrightStor® ARCserve Backup for Laptops & Desktops to restore data and with Unicenter® Desktop DNA® to restore personal settings and configurations.
- **Automatic Patch Re-deployment.** Based on policies, post-requirements and other automation features.

Administration and Management. Unicenter Patch Management enables the administrator to direct and control the complex patch management process with an easy to use task orientated user interface. This interface, combined with the web reporting portal, provides the controls and information required for comprehensive administration and management of the entire patch management process.

- **Intuitive and Task Orientated User Interface.** Patch management functions are wizard driven and context relevant for the functional role of user type.
- **Customizable Interface.** The interface is customizable by each user, allowing for personal preferences and desired information pane. (See Figure 3)
- **Web-based Report Portal.** Wizard-driven reporting to incorporate user role and interest, with automatic report scheduling per policy with distribution of alerts and affected assets.

Supported Environments

- Windows XP
- Windows 2000
- Windows 2003

For more information, call 1-888-864-2368 or visit ca.com