Ethical Hacking and Countermeasures

Version 6

Module LXV

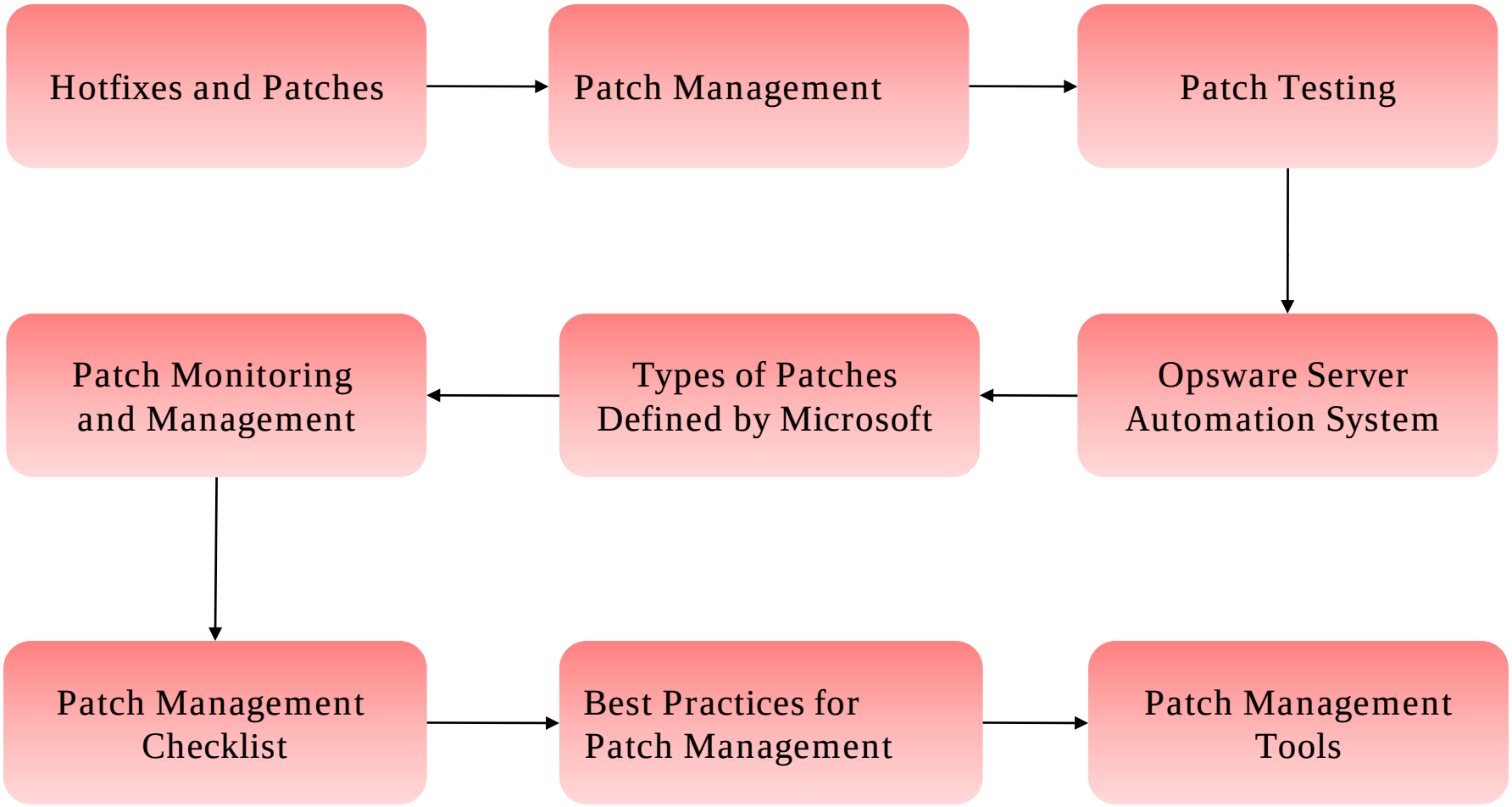
Patch Management

Module Objective

This module will familiarize you with:

- Hotfixes and Patches
- Patch management
- Patch Testing
- Understanding Patch Monitoring and Management
- Types of Patches Defined by Microsoft
- Opsware Server Automation System (SAS)
- Patch Management Checklist
- Best Practices for Patch Management
- Patch Management Tools

Module Flow



Hotfixes and Patches

A hotfix is a code that fixes a bug in a product. The users may be notified through emails or through the vendor's website

Hotfixes are sometimes packaged as a set of fixes known as combined hotfix or service pack

A patch can be considered as a repair job in a piece of programming problem. A patch is the immediate solution provided to users

What is Patch Management

"Patch management is a process to ensure that the appropriate patches are installed on a system"

It involves:

- Choosing, verifying, testing, and applying patches
- Updating previously applied patches with current patches
- Listing patches applied previously to the current software
- Recording repositories, or depots, of patches for easy selection
- Assigning and deploying applied patches

Patch Testing

The first step in patch testing is the verification of patch source and integrity which helps you to ensure that update is valid and it is not altered

The major components of patch testing include:

- Digital signatures
- Checksums
- Integrity verification

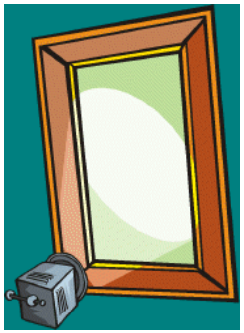
Patch testing process takes place in three different categories:

- Testing Patch Installation
- Testing Application Patches
- Testing Service Patches

Understanding Patch Monitoring and Management

Steps in the Patch Management framework are as follows:

1. Identify the patch location
2. Identify new patches and verify the patch's authenticity by installing each patch on an isolated system, and determine the time frame
3. Ensure that both patch testing and risk assessment of patch deployment are processed at one place
4. Deploy the patch



Understanding Patch Monitoring and Management (cont'd)

Create a Change Process:

- Creating a change management process is like updating software that is required for a system
- Before starting the change management process, switch off the server, and start the process from a small log

Monitor the Patch Process:

- Microsoft suggested a four phase approach that monitors the software updates designed for the management control:
  - Assess
  - Identify
  - Evaluate and Plan
  - Deploy

Types of Patches Defined by Microsoft

Microsoft releases patches to facilitate updates to the Windows OS and Microsoft applications

- Such patches fix known problems, or bugs, in an OS or application and are shipped in three formats:

Hotfixes

- A code that fixes a bug in a product
- Also referred as security fixes or Quick Fix Engineering (QFE) Fixes

Roll-ups

- Merges updates of several Hotfixes into a single update file

Service packs

- An update to a software version that fixes a bug
- Include fixes not previously released and introduces new functionality

Opsware Server Automation System (SAS)

Opsware Server Automation System (SAS) is the data center automation product of choice for heterogeneous IT environments

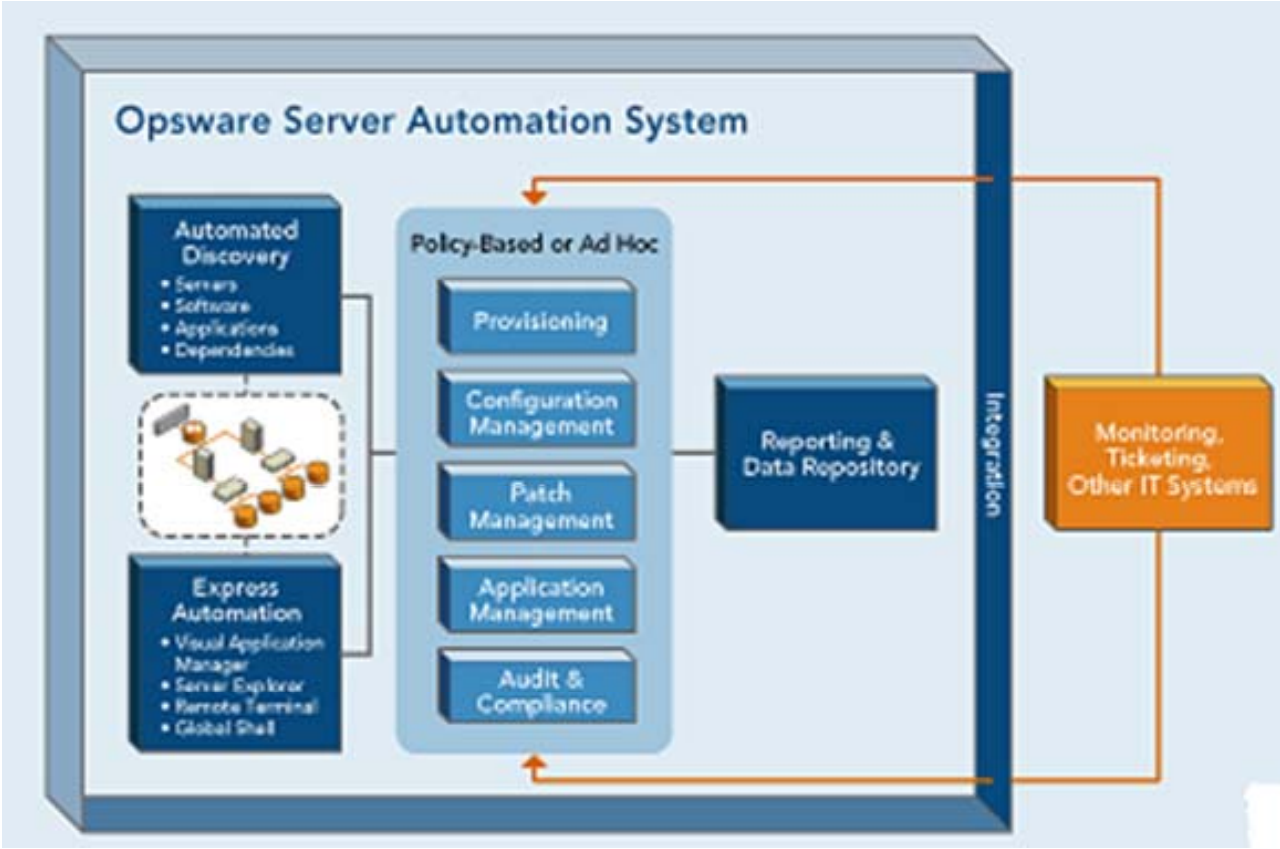
It gives administrators the ability to monitor systems and apply configuration changes across many servers in a uniform fashion

Servers can be provisioned from the same pre-defined baseline from the start

Configuration tracking is used to detect changes that are made and administrators are notified of the changes

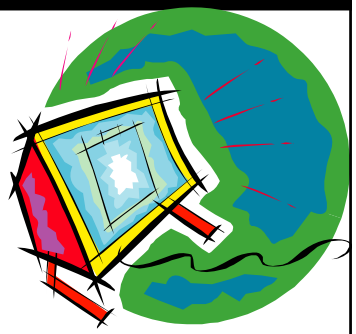
The administrator can then use Opsware to rollback the change or propagate the change throughout the server environment

Opsware Server Automation System (SAS) (cont'd)



Patch Management Tools

Tool: UpdateExpert

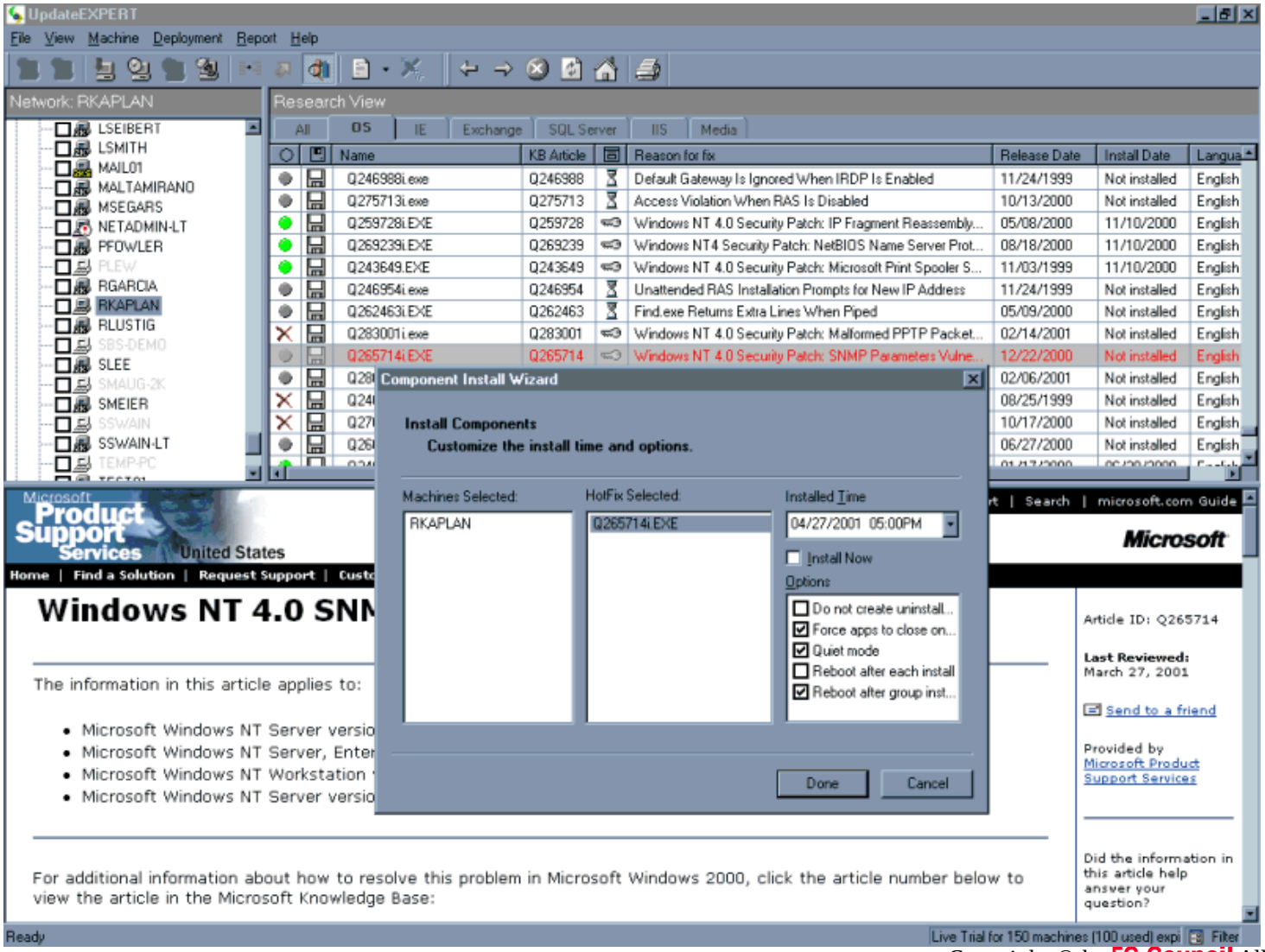


UpdateExpert is a Windows administration program that helps you to secure your systems by remotely managing service packs and hotfixes

Microsoft constantly releases updates for the OS and mission critical applications, which fix security vulnerabilities and system stability problems

UpdateExpert enhances security, keeps systems up-to-date, eliminates sneaker-net, improves system's reliability and QoS

UpdateExpert: Screenshot



Tool: Qfecheck

Qfecheck allows customers to diagnose and eliminate the effects of anomalies in the packaging of hotfixes for Microsoft Windows

Qfecheck.exe determines which hotfixes are installed by reading the information stored in the following registry key:

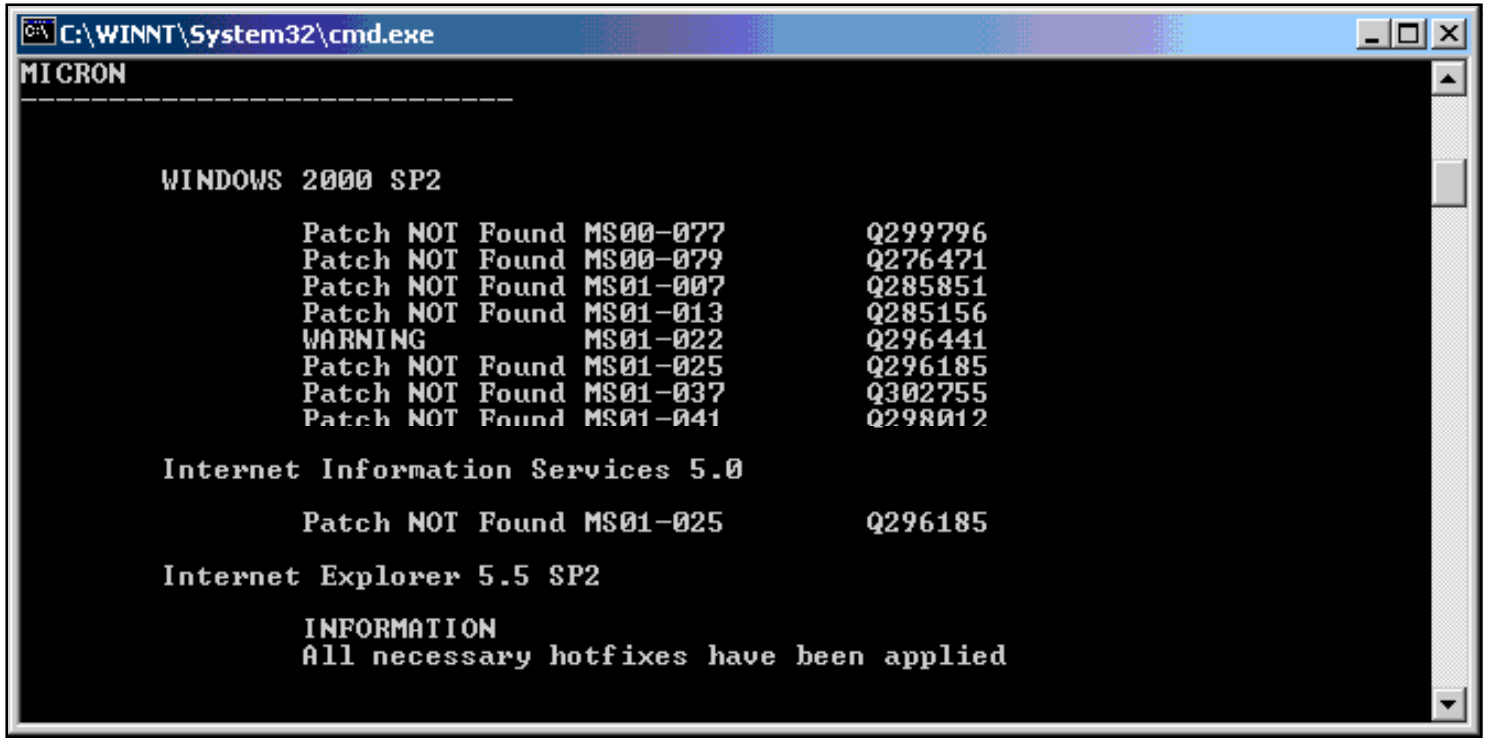
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Updates


```
G:\CEH\Haja\patch>qfecheck /v

Windows 2000 Hotfix Validation Report for \\SYSTEM5
Report Date: 5/17/2005  2:23pm

Current Service Pack Level:  Service Pack 4

Hotfixes Identified:
Q327194:  Current on system.
KB820888:  Current on system.
KB822831:  Current on system.
KB823182:  Current on system.
KB823559:  Current on system.
KB824105:  Current on system.
KB825119:  Current on system.
KB826232:  Current on system.
KB828035:  Current on system.
KB828741:  Current on system.
KB828749:  Current on system.
KB835732:  Current on system.
KB837001:  Current on system.
KB839645:  Current on system.
KB840315:  Current on system.
KB840987:  Current on system.
KB841356:  Current on system.
KB841533:  Current on system.
KB841872:  Current on system.
KB841873:  Current on system.
KB842526:  Current on system.
KB842773:  Current on system.
KB871250:  Current on system.
KB873333:  Current on system.
KB873339:  Current on system.
KB885250:  Current on system.
KB885835:  Current on system.
KB885836:  Current on system.
KB888113:  Current on system.
KB890047:  Current on system.
KB890175:  Current on system.
KB890859:  Current on system.
KB891711:  Current on system.
KB891781:  Current on system.
KB893066:  Current on system.
KB893086:  Current on system.
KB893803:  Current on system.
Q818043:  Current on system.
```

Tool: HFNetChk

HFNetChk is a command-line tool that enables the administrator to check the patch status of all the machines in a network remotely

It does this function by referring to an XML database that Microsoft constantly updates

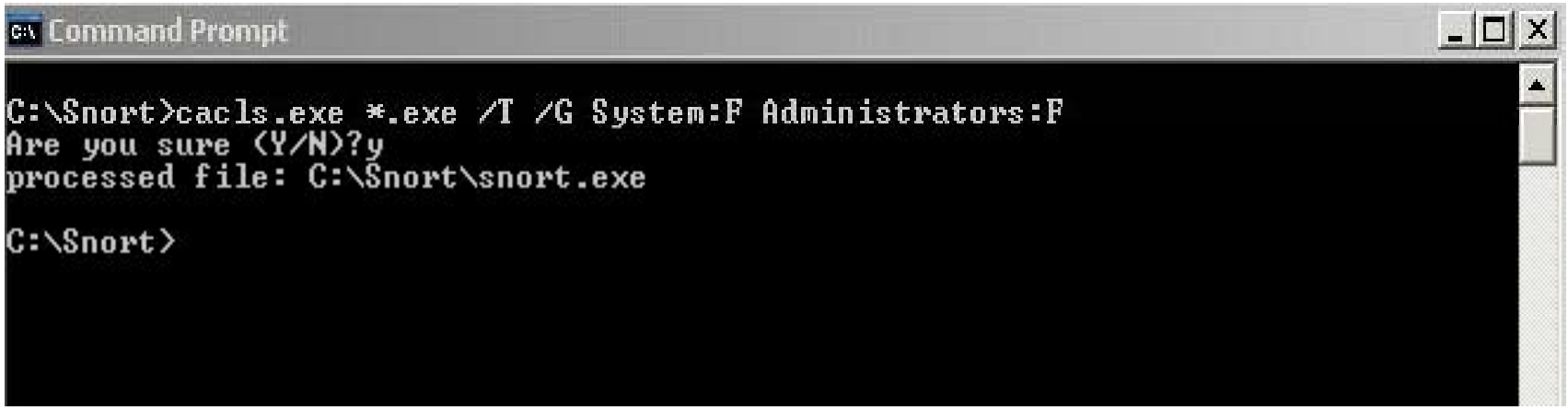


cacls.exe Utility

Built-in Windows 2000 utility (cacls.exe) can set access control list (ACLs) permissions globally

To change permissions on all executable files to System:Full, Administrators:Full:

- `C:\>cacls.exe c:\myfolder\*.exe /T /G System:F Administrators:F`



Tool: Shavlik NetChk Protect

Shavlik NetChk protect is a tool that automates the management of critical security patches, spyware, malware, and unwanted software applications from one console

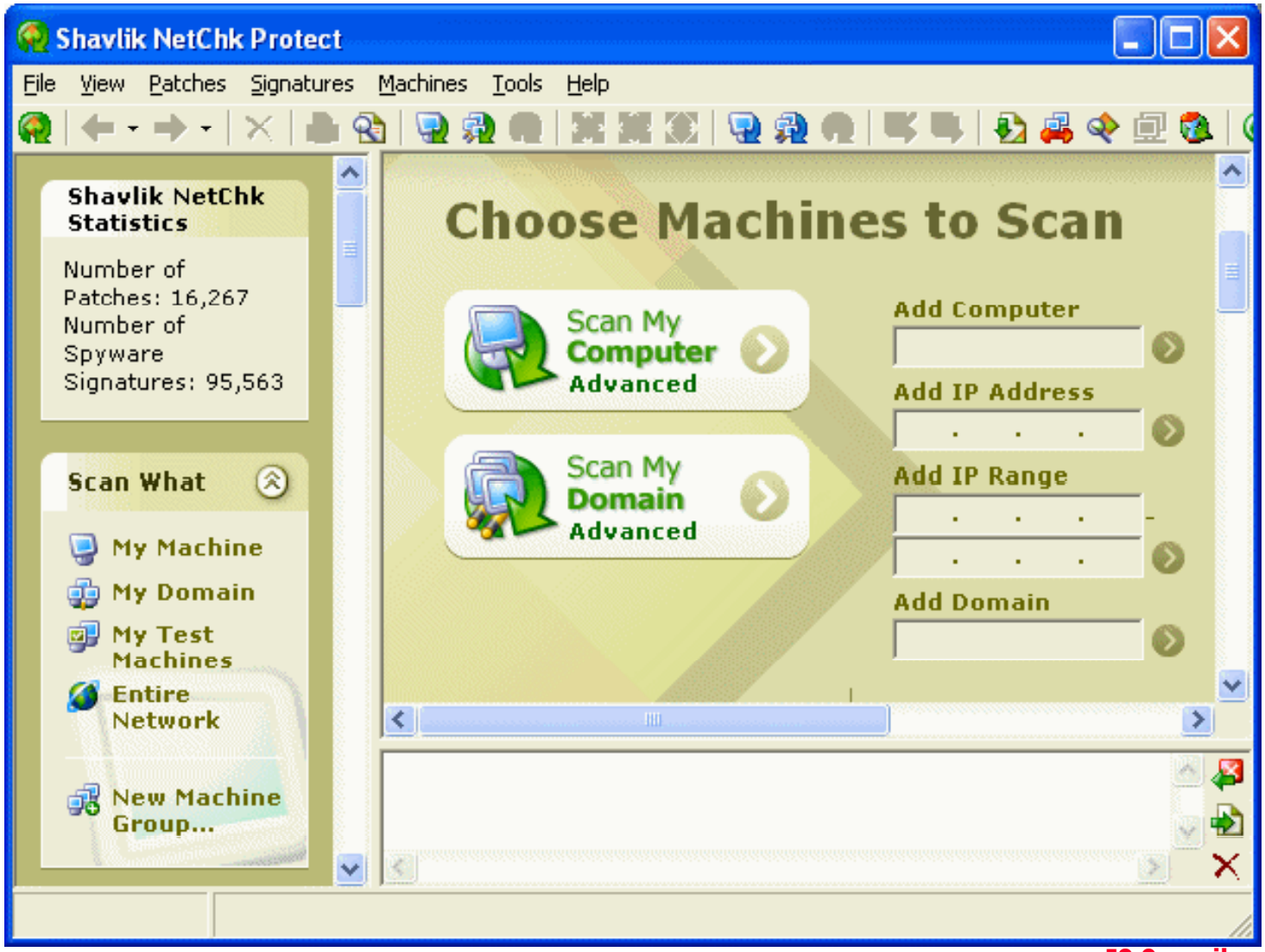
It offers a solution for detecting, removing, and managing critical threats and vulnerabilities with active vulnerability management

Maintain secure, policy-compliant networks through automatic and continuous assessment, remediation, and management

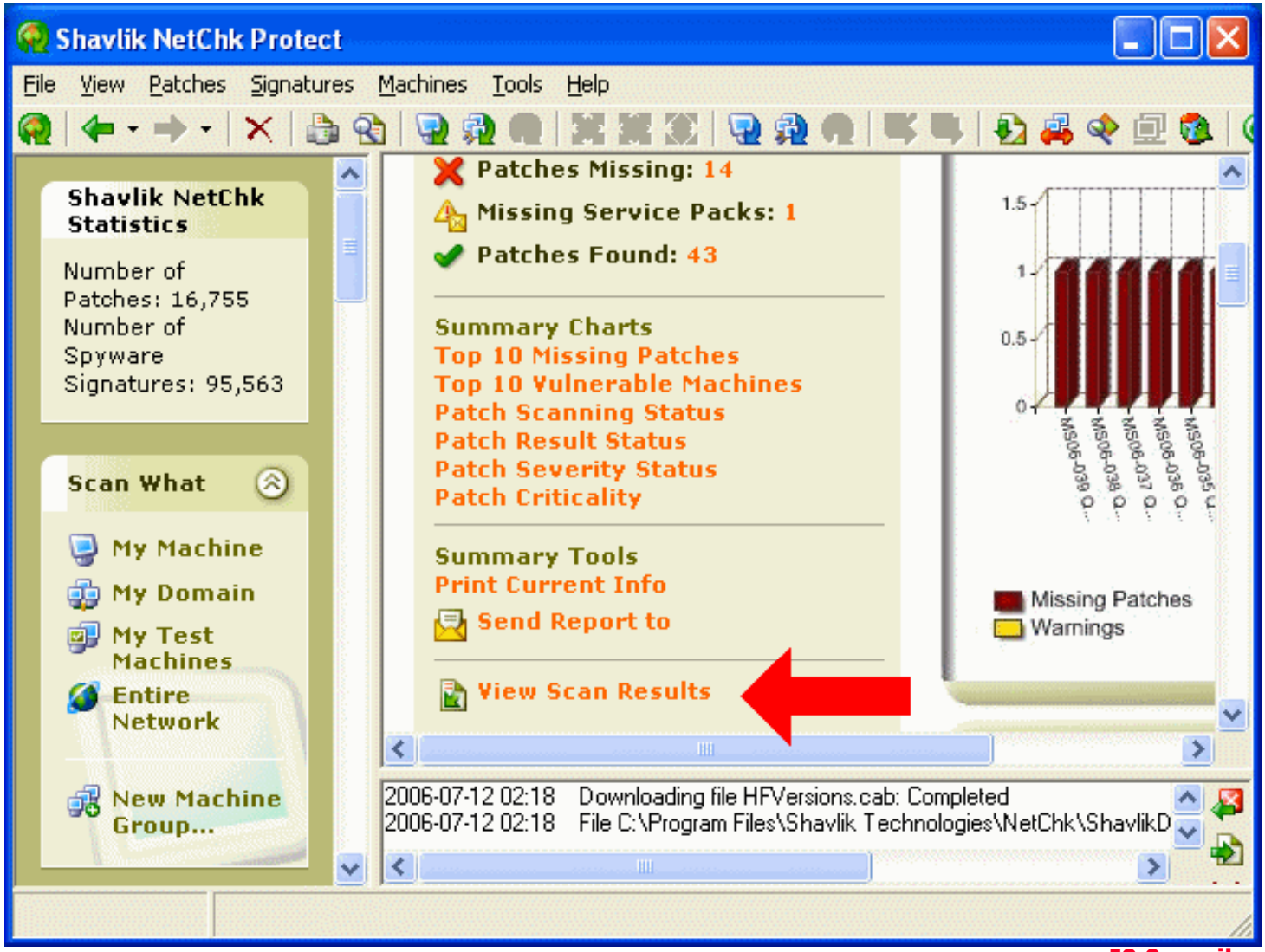
Features:

- Patch Scanning
- Extensive Reporting
- Patch development
- Spyware Management
- Desktop Application Control

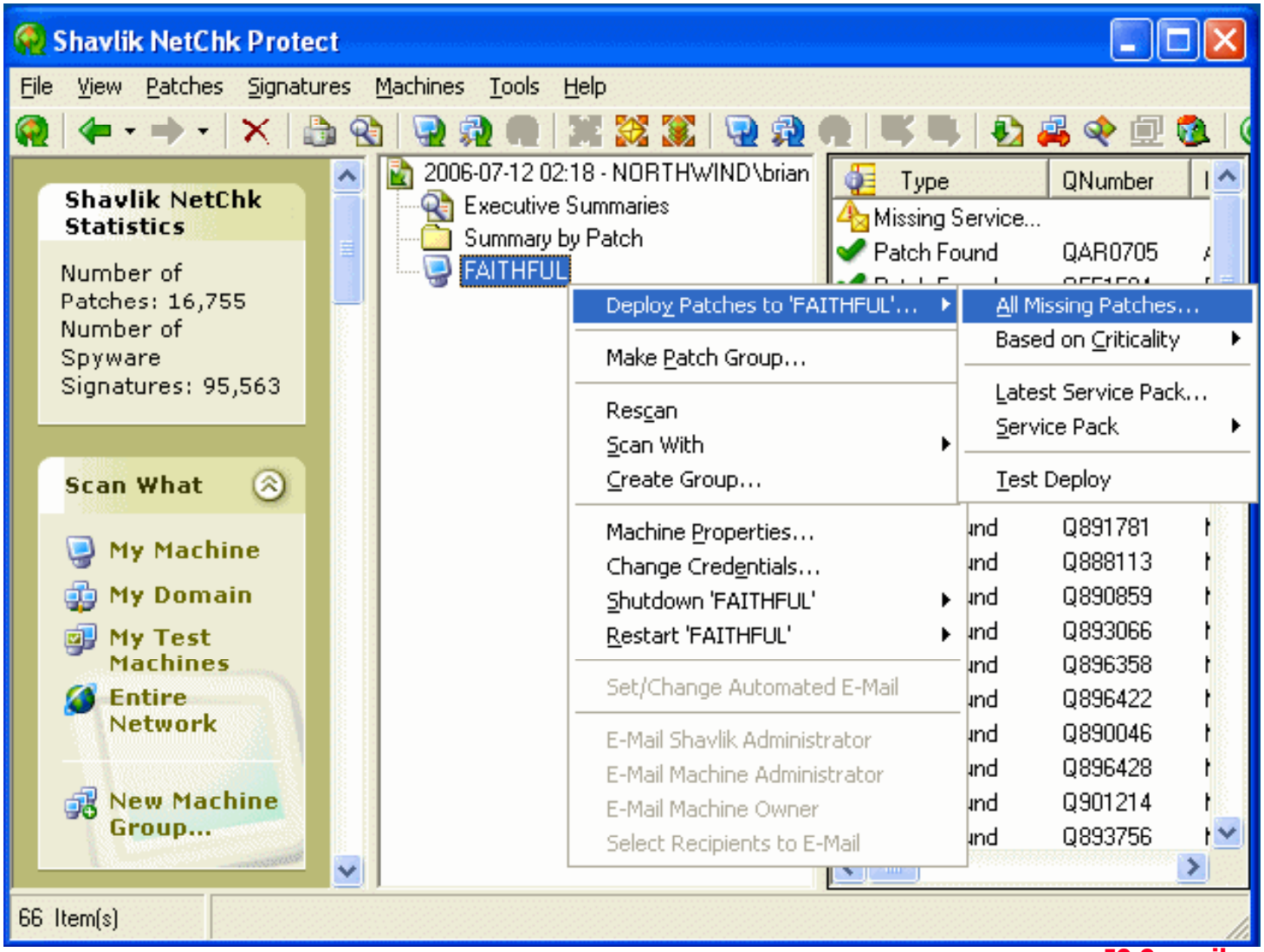
Shavlik NetChk Protect: Screenshot 1



Shavlik NetChk Protect: Screenshot 2



Shavlik NetChk Protect: Screenshot 3



Tool: Kaseya Patch Management

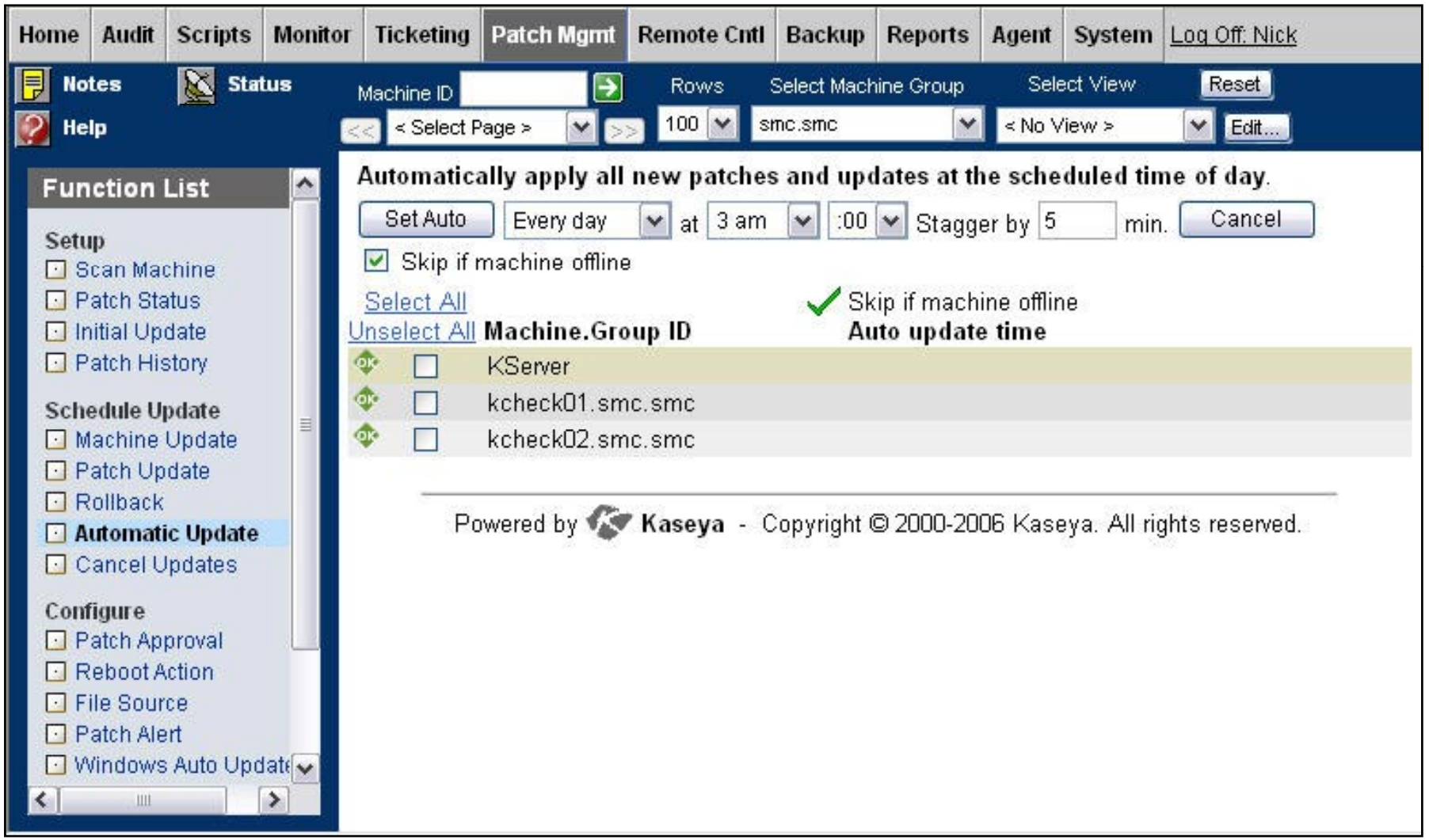
Kaseya Patch Management is used to keep your servers, workstations, and remote computers up-to-date with the latest security patches and updates

It provides the automatic discovery of all missing patches and updates

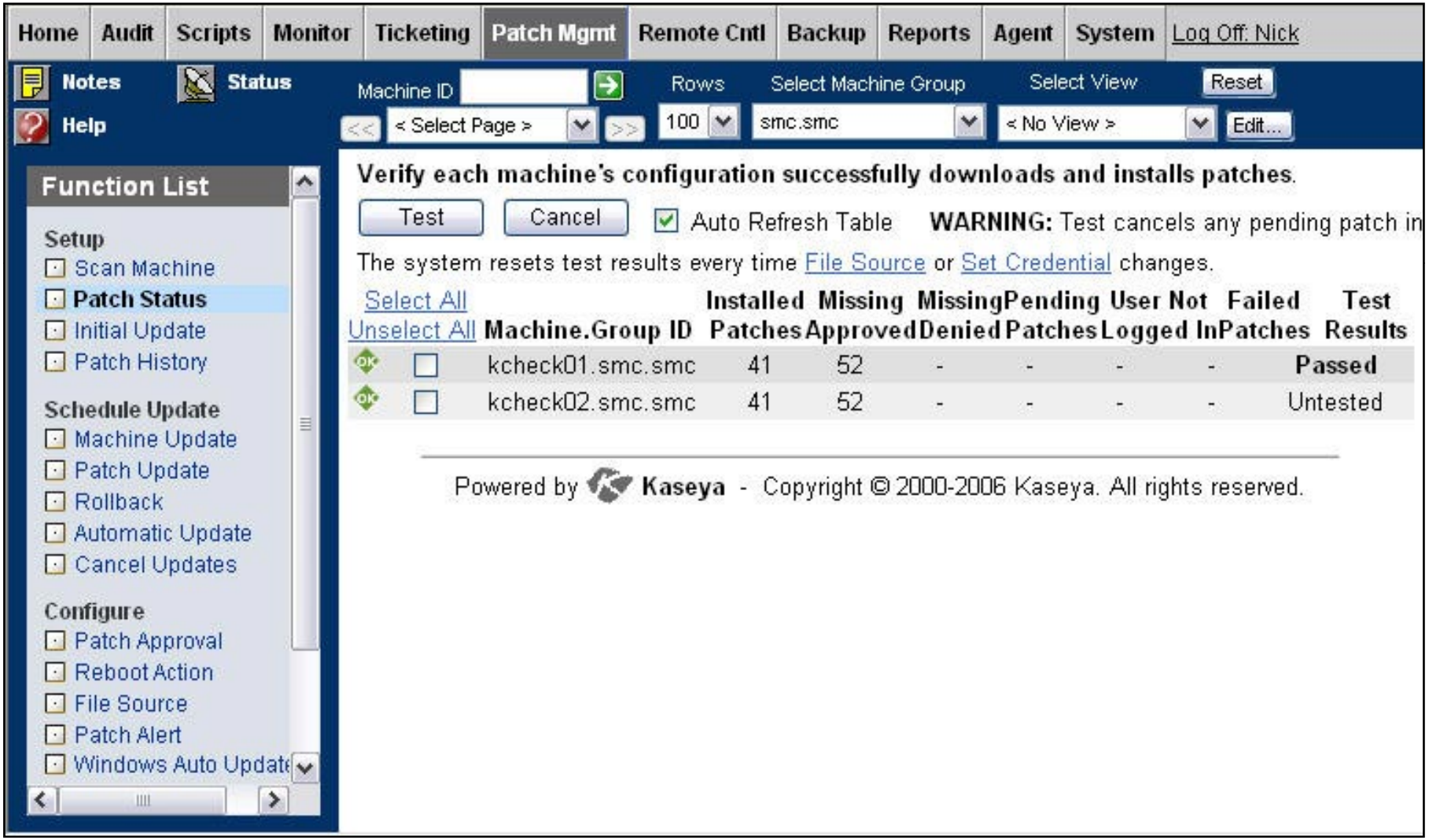
Features:

- Complete automation for patch discovery and deployment patch
- Location, deployment method, and parameter control reliable and up to date patch data base
- Complete rollback
- Comprehensive history and reporting
- Rapid deployment

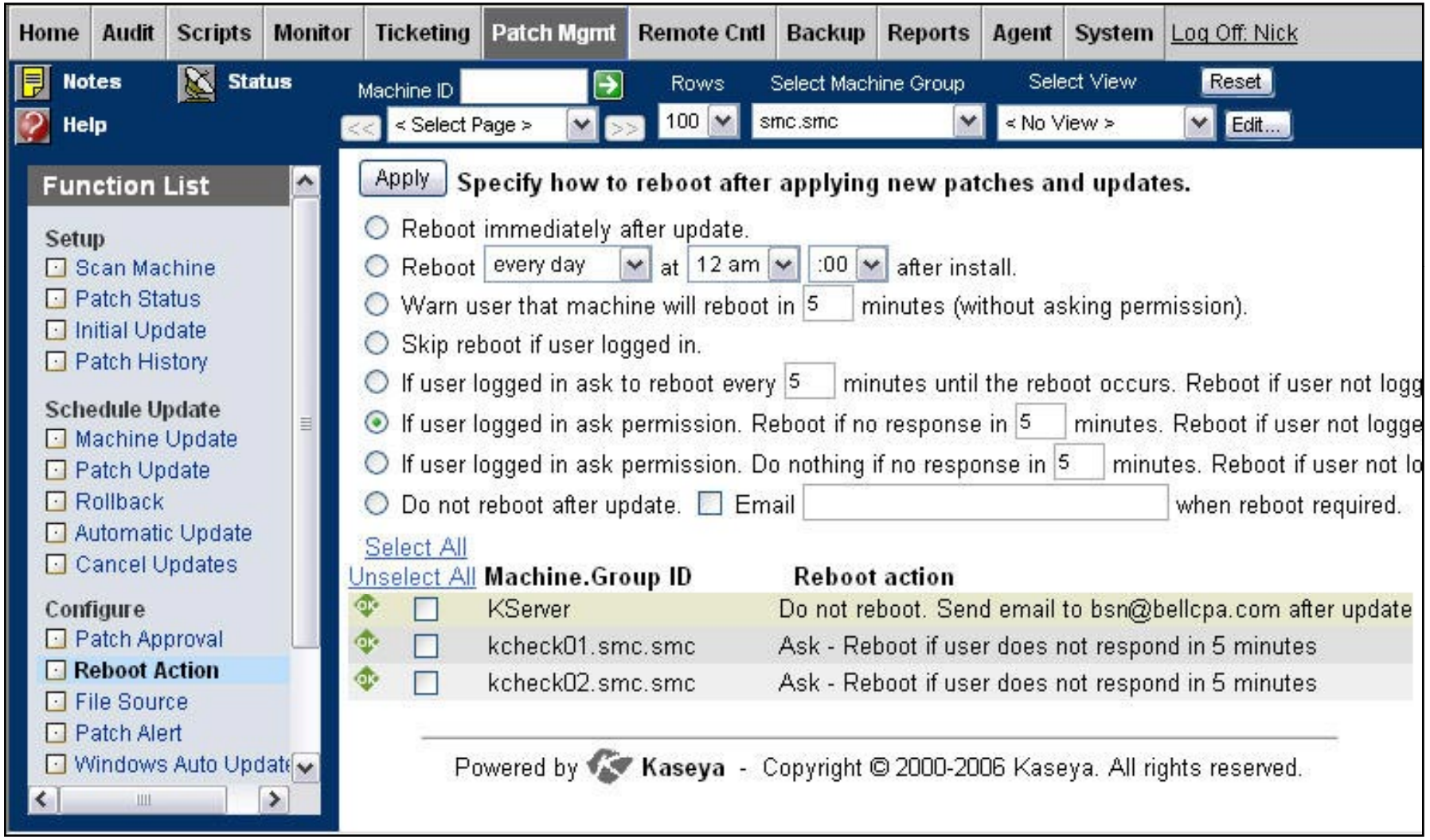
Kaseya Patch Management: Screenshot 1



Kaseya Patch Management: Screenshot 2



Kaseya Patch Management: Screenshot 3



Tool: IBM Tivoli Configuration Manager

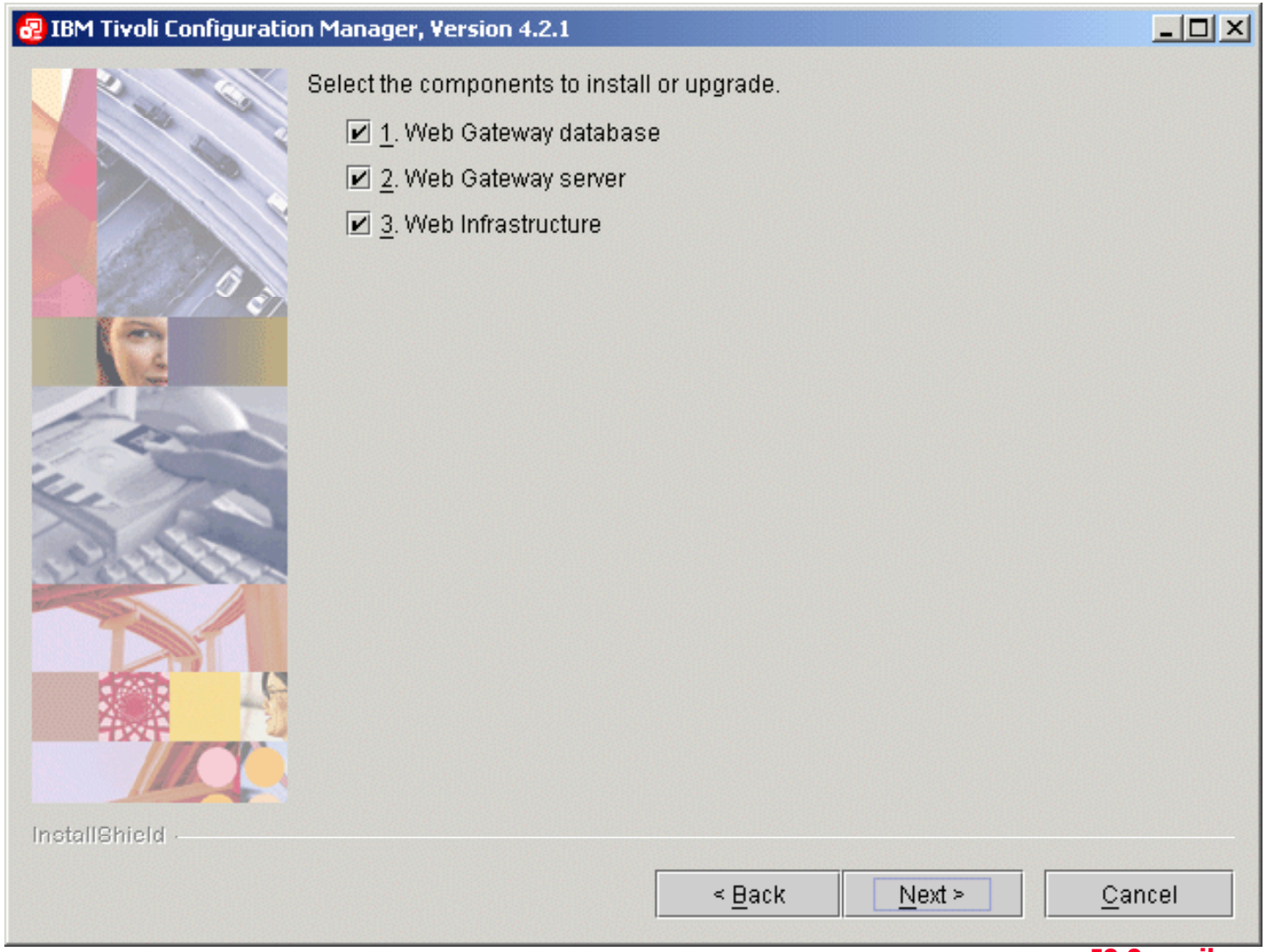
IBM's configuration manager provides Microsoft client and server software patch automation capabilities in distributed environments

Obtains, packages, distributes, and installs Microsoft software patches needed by client systems in distributed customer environments

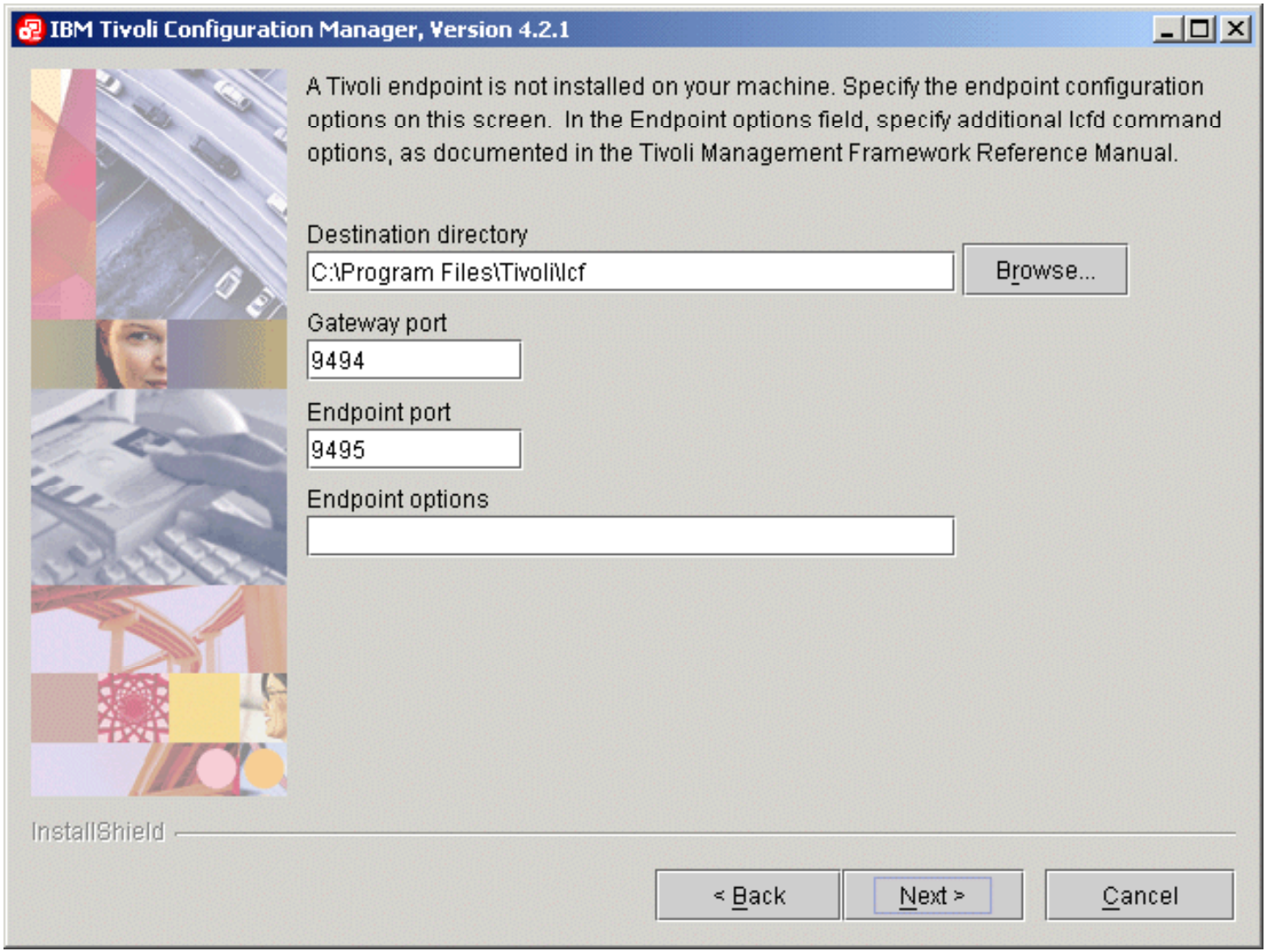
Features:

- Gathers software patch signature files and distributes them to client machines
- Scans clients
- Determines missing patches
- Packages patches
- Builds patch deployment plans
- Distributes required patches to clients

IBM Tivoli Configuration Manager: Screenshot 1



IBM Tivoli Configuration Manager: Screenshot 2



Tool: LANDesk Patch Manager

LANDesk's Patch Manager includes a subscription service that collects and analyzes patches for heterogeneous environments

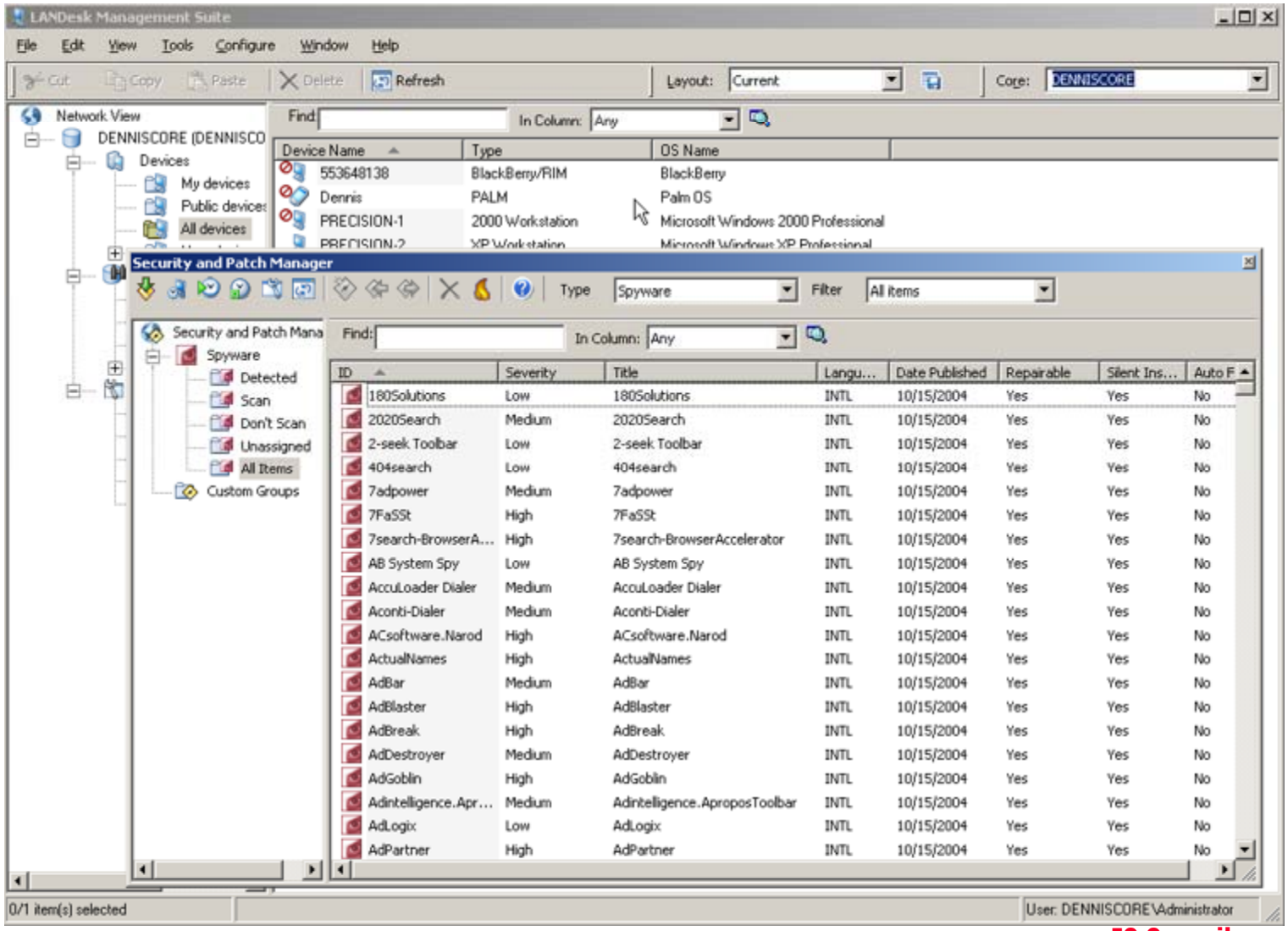
It scans managed devices to identify application and operating system vulnerabilities

It monitors the status of each install and provides bandwidth throttling, staging, and detailed policy and compliance reporting across a broad range of operating systems

It increases productivity by evaluating systems with active vulnerability scanning

It is used to gain control with a single tool to research, review, and download available patches

LANDesk Patch Manager: Screenshot



Tool: ConfigureSoft Enterprise Configuration Manager (ECM)

ECM centralizes and automates the monitoring, managing and auditing of hardware and software configurations across Windows, UNIX, and Linux platforms

It automatically discovers new systems and tracks configuration changes at scheduled intervals to ensure the availability of the latest patch information is available

Features:

- Vulnerabilities assessment and remediation
- Regulatory & operational compliance
- Configuration management & control
- Change management
- Risk prevention and security management
- System optimization

ConfigureSoft Enterprise Configuration Manager (ECM): Screenshot

Tool: BladeLogic Configuration Manager

BladeLogic Configuration Manager is a component of the BladeLogic Operations Manager suite of data center automation products

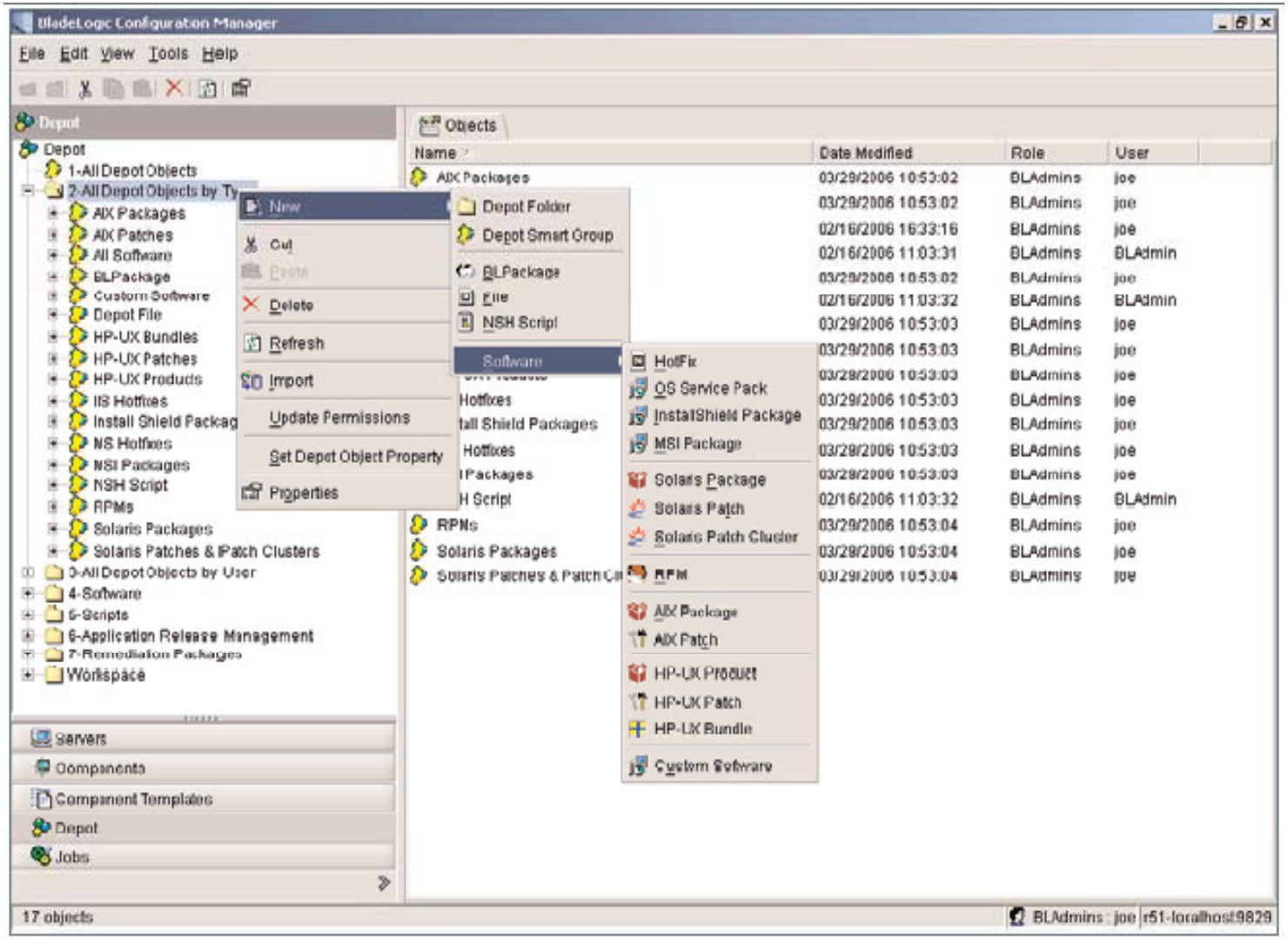
It features a cross-platform command line interface that supports a single-sign on using a range of authentication protocols

It supports a policy-based approach whereby changes are applied to a policy, and then synchronized with the target servers

All user communication is encrypted, and all user actions are logged and can be authorized based on a user's role

It allows IT organizations to monitor, patch, configure, and update servers across platforms and data centers

BladeLogic Configuration Manager: Screenshot



Tool: Microsoft Baseline Security Analyzer (MBSA)

Microsoft baseline security analyzer determines critical updates and the required updates on the target computer

It scans for common security mis-configuration errors on target computers

It supports two interface for scanning:

- GUI Scan (Mbsa.exe)
- Command Line Interface (Mbsacli.exe)

MBSA: Scanning Updates in GUI Mode

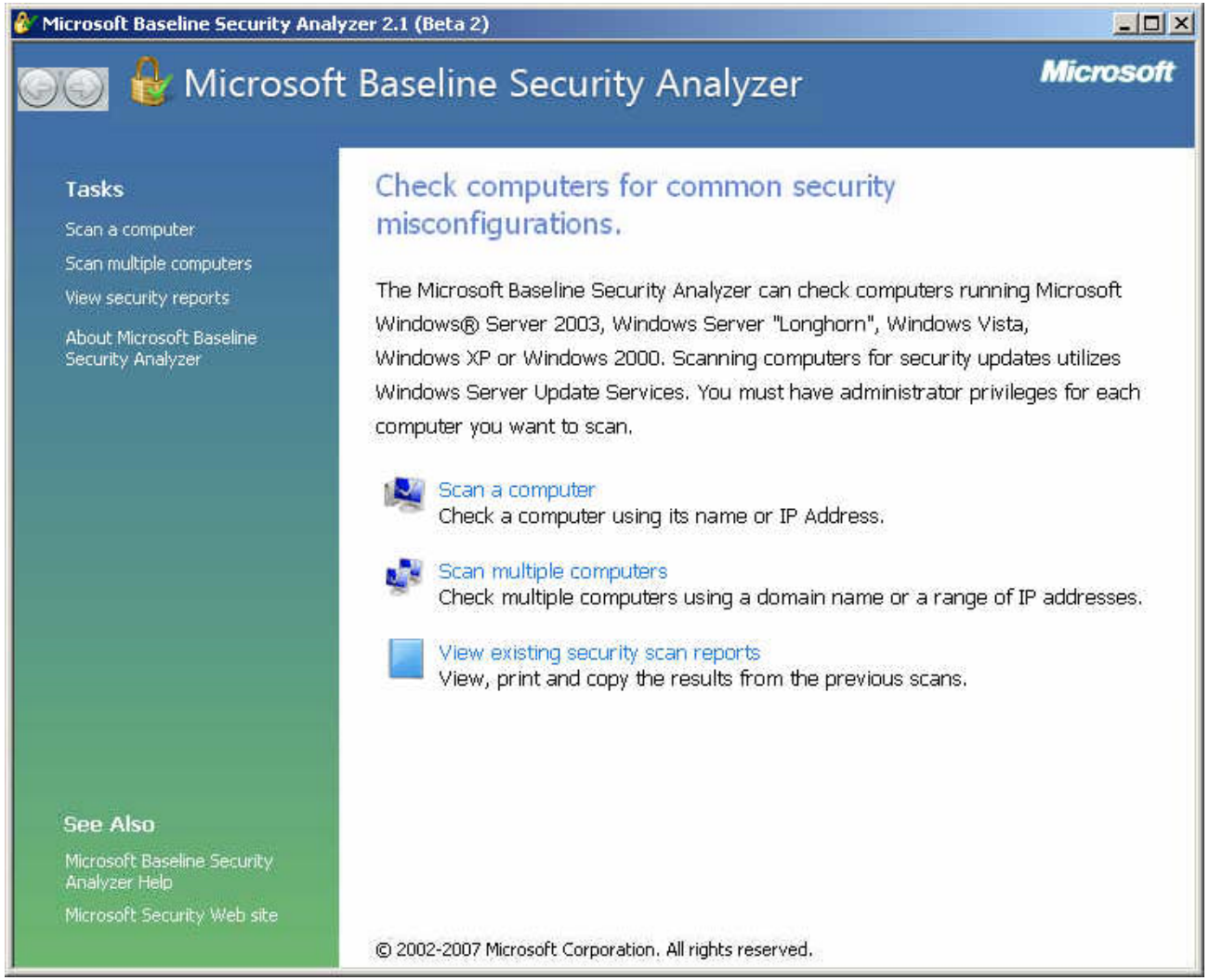
MBSA defines scanning options and displays the results of the security scan in the MBSA window

It scans and reports on updates designated as critical security updates by the Windows Update site

Procedure:

- Open MBSA
- Enable the check For security updates option
- Scan completion display XML file for the respective computer

MBSA: Screenshot



MBSA: Scanning Updates in Command-line Version

The MBSA command line interface supports two types of scan namely:

MBSA-style scan

```
•mbsacli [/c|/i|/r|/d domainname|ipaddress|ipaddressrange]
 [/n option] [/sus SUS server|SUS filename] [/s level]
 [/nosum] [/nvc] [/o filename] [/e] [/l] [/ls] [/lr report
 name] [/ld report name] [/v] [/?] [/qp] [/qe] [/qr] [/q]
 [/f] [/unicode]
```

HFNetChk-style scan

```
•mbsacli /hf [-h hostname] [-fh filename] [-i ipaddress] [-
 fip filename] [-r ipaddressrange] [-d domainname] [-n] [-sus
 SUS server|SUS filename] [-fq filename] [-s 1] [-s 2] [-
 nosum] [-sum] [-z] [-v] [-history level] [-nvc] [-o option]
 [-f filename] [-unicode] [-t] [-u username] [-p password] [-
 x] [-?]
```

Tool: QChain

Qchain allows to install multiple security updates

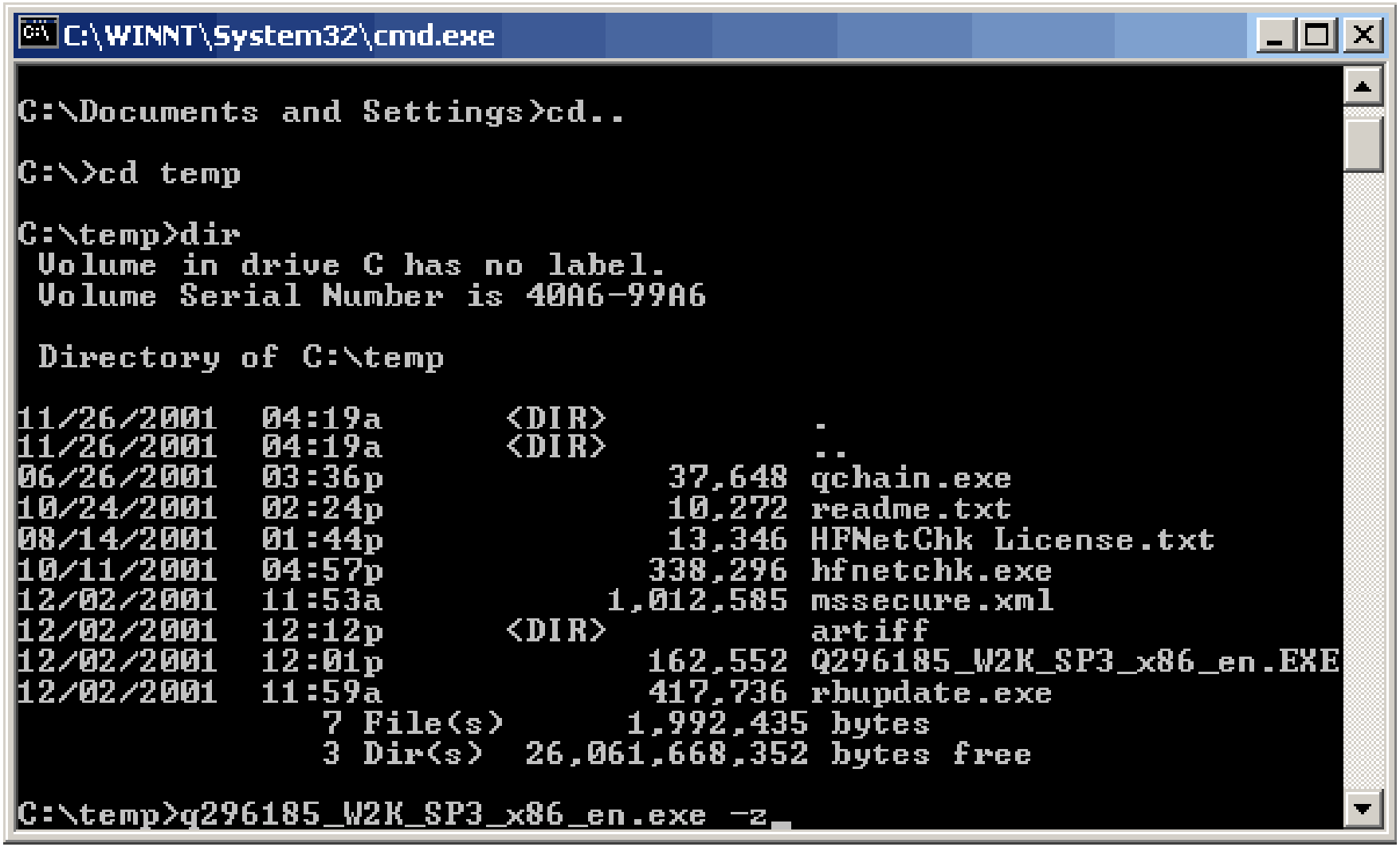
It evaluates the drivers, DLLs, and executable files updated by each security update

It creates a batch file for the security update installation

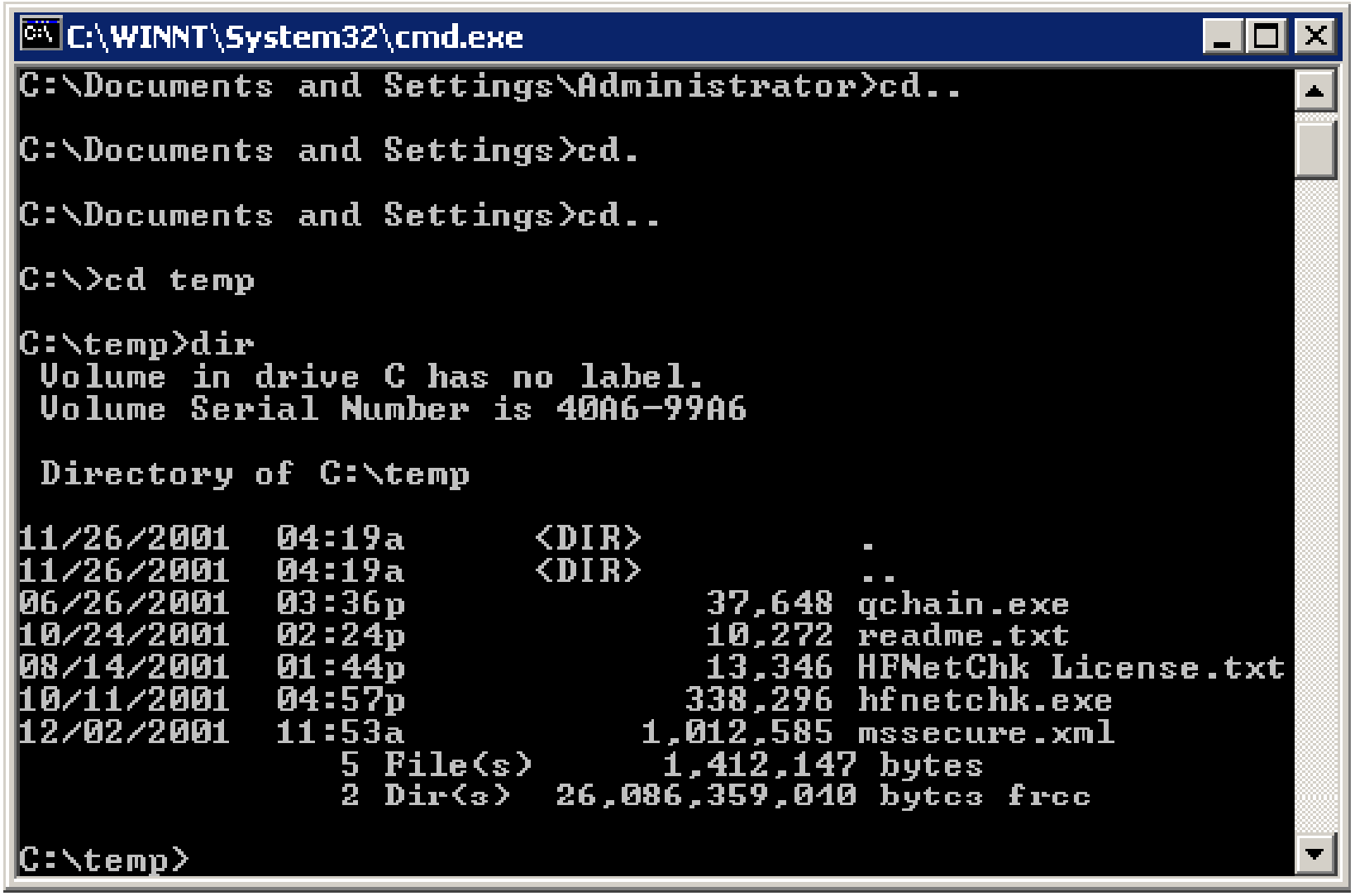
Batch file installs each security update with:

- -z switch to prevent reboots after each security update installation
- -m switch to enable unattended installs

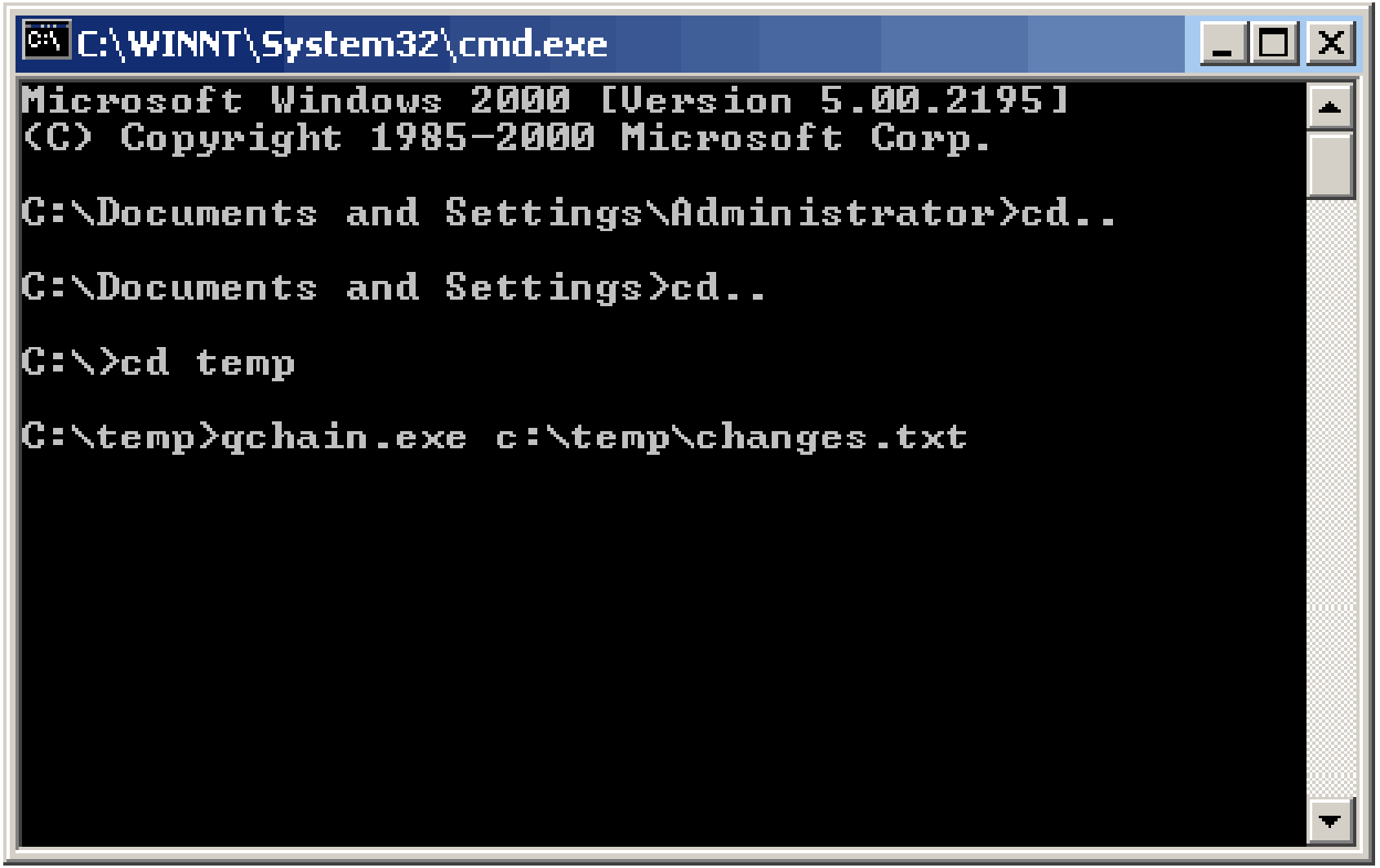
Qchain: Screenshot 1



Qchain: Screenshot 2



Qchain: Screenshot 3



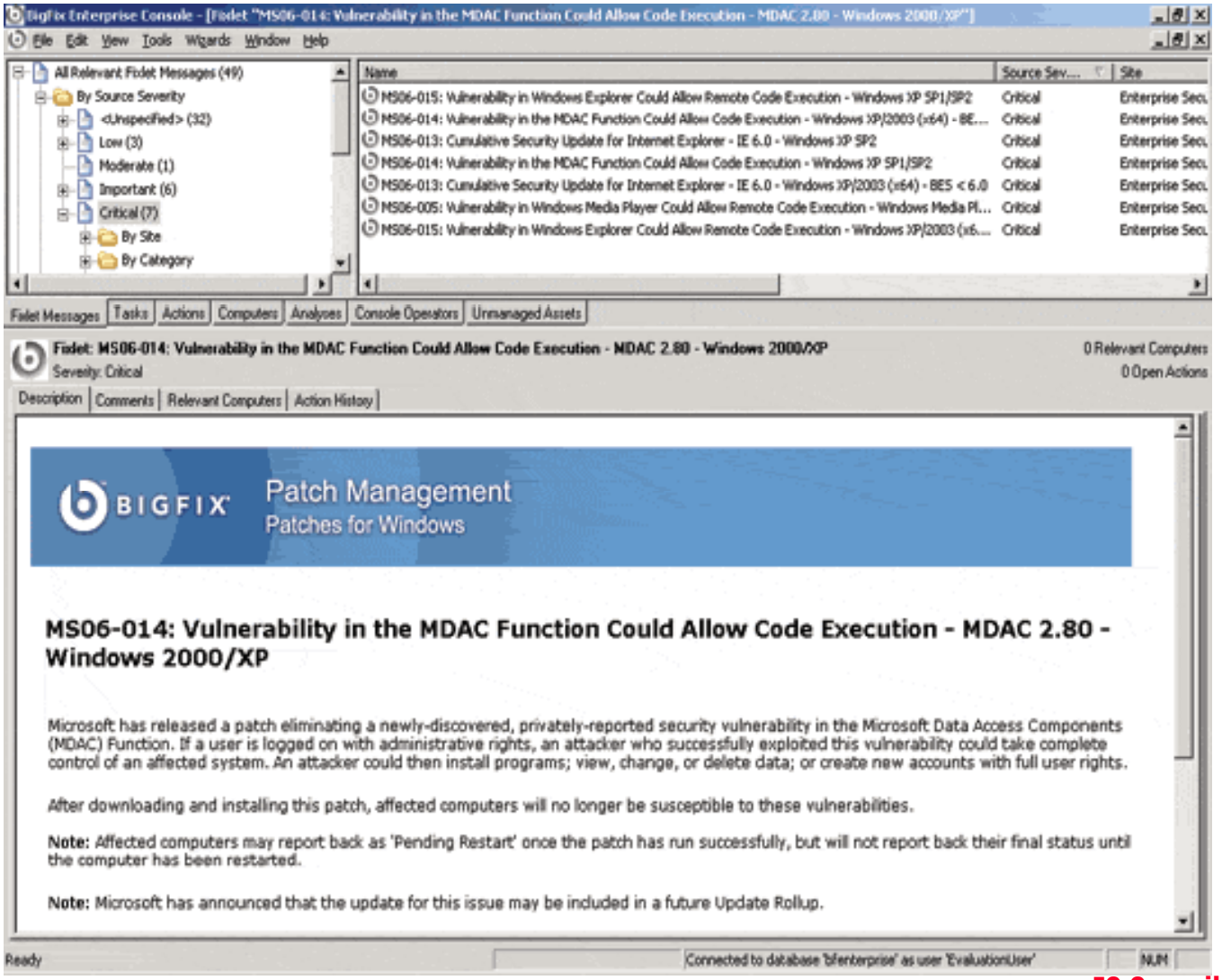
Tool: BigFix Enterprise Suite (BFS)

BigFix Enterprise Suite platform provides patch management solution for distributed and multiplatform networks

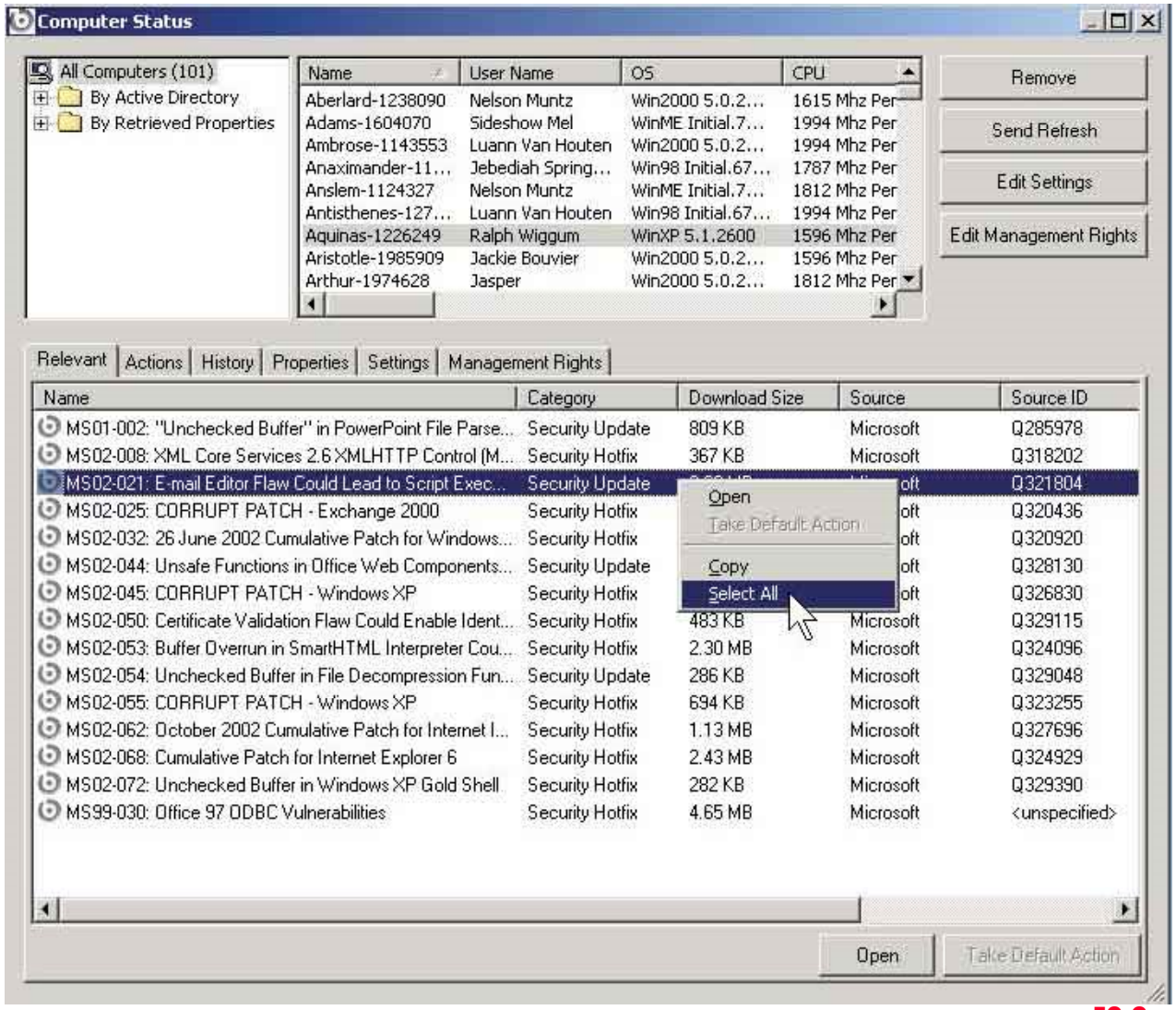
Roll back feature helps in securing the system in case of patches that misfire

It enables audit trial of every action and step taken on each computer during the patch management process

BigFix Enterprise Suite (BFS): Screenshot 1



BigFix Enterprise Suite (BFS): Screenshot 2



Tool: Shavlik NetChk Protect

Shavlik NetChk protect is a patch management solution for larger networks and organizational units

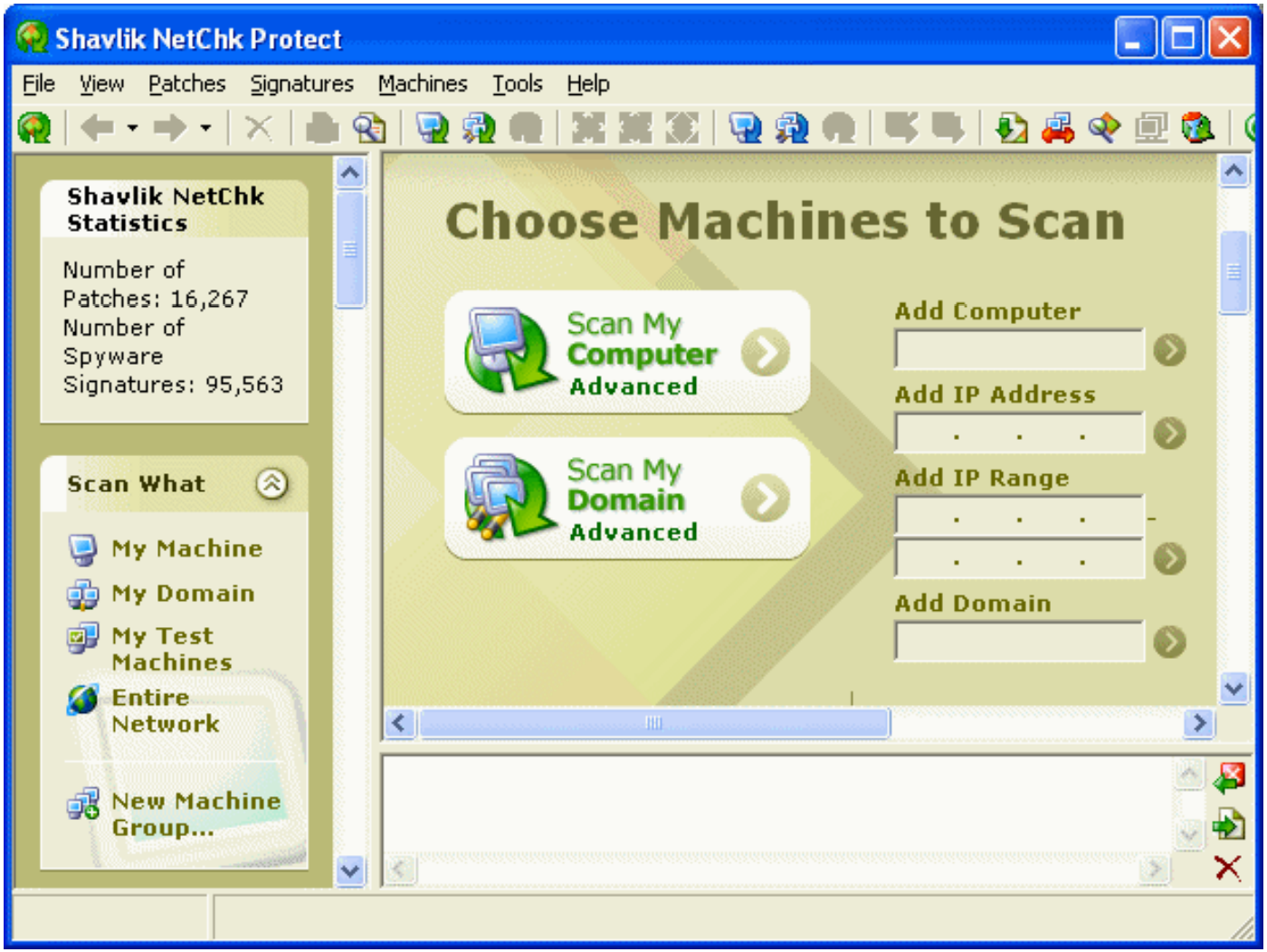
Features:

- Drag-n-Drop patch management interface controlled by the user enables scanning of the required groups
- Security configuration management mitigates organizational costs and provides the security associated with the expensive breaches
- It automates the platforms and products such as Windows NT, XP,2000, etc

Benefits:

- Performs scheduled scans
- Uses options such as Command line scanning and scanning and deployment with SQL server database

Shavlik NetChk Protect: Screenshot



Tool: PatchLink Update

PatchLink Update is a patch and vulnerability solution for large networks

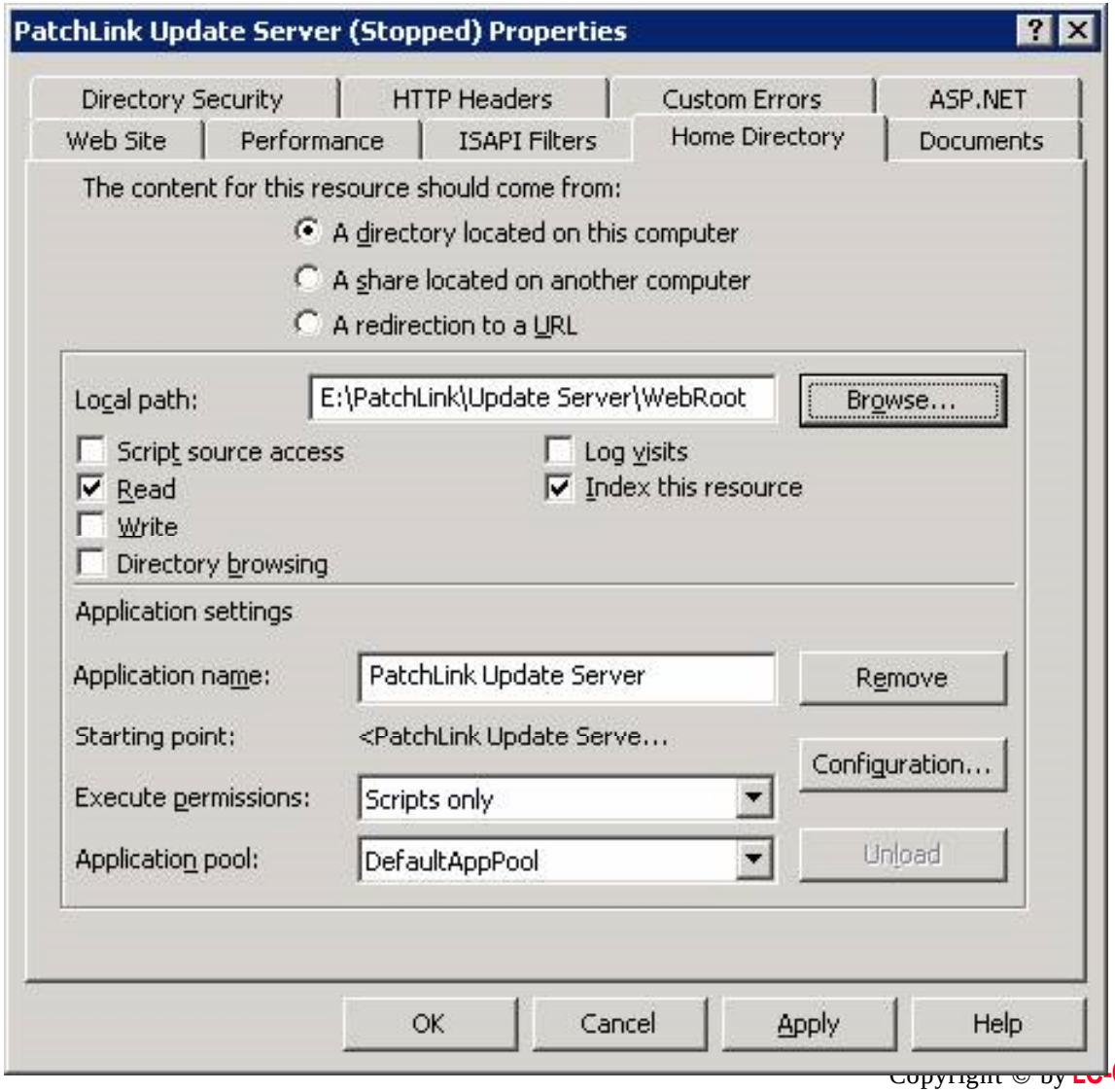
It scans networks for security holes using fingerprint technology

It translates security policies into automated and continuous protection against network vulnerabilities

Features:

- Customized subscription notifications to include the required platforms and languages
- Improved transaction/query efficiency that increases performance and scalability
- Proxy server authentication that increases deployment security

PatchLink Update: Screenshot



Tool: SecureCentral PatchQuest

SecureCentral PatchQuest is a web-based patch management software that manages and distributes security patches across various platforms

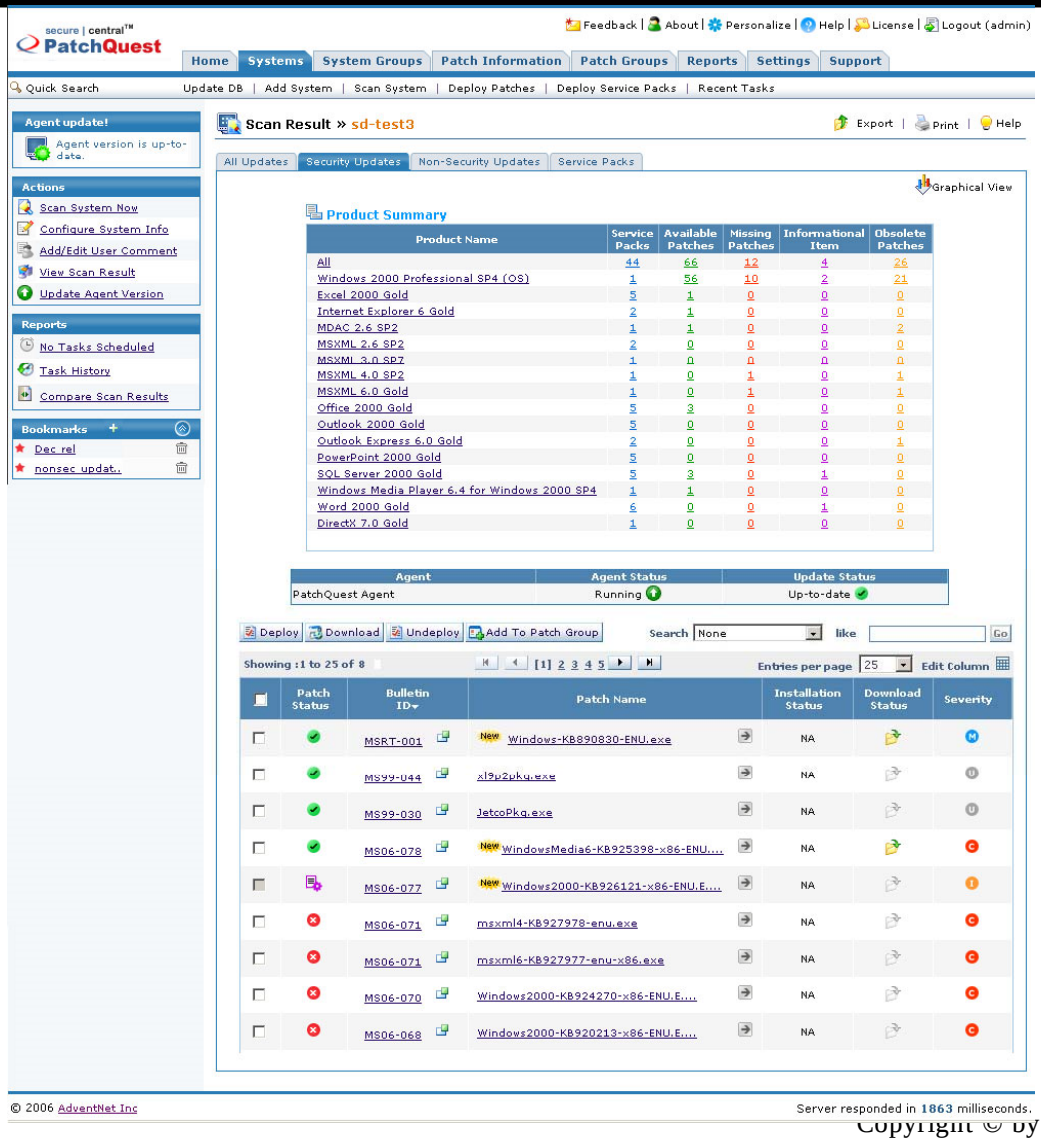
Four stages in working:

- System addition & discovery
- Patch assessment or scanning
- Patch download and deployment
- Reporting

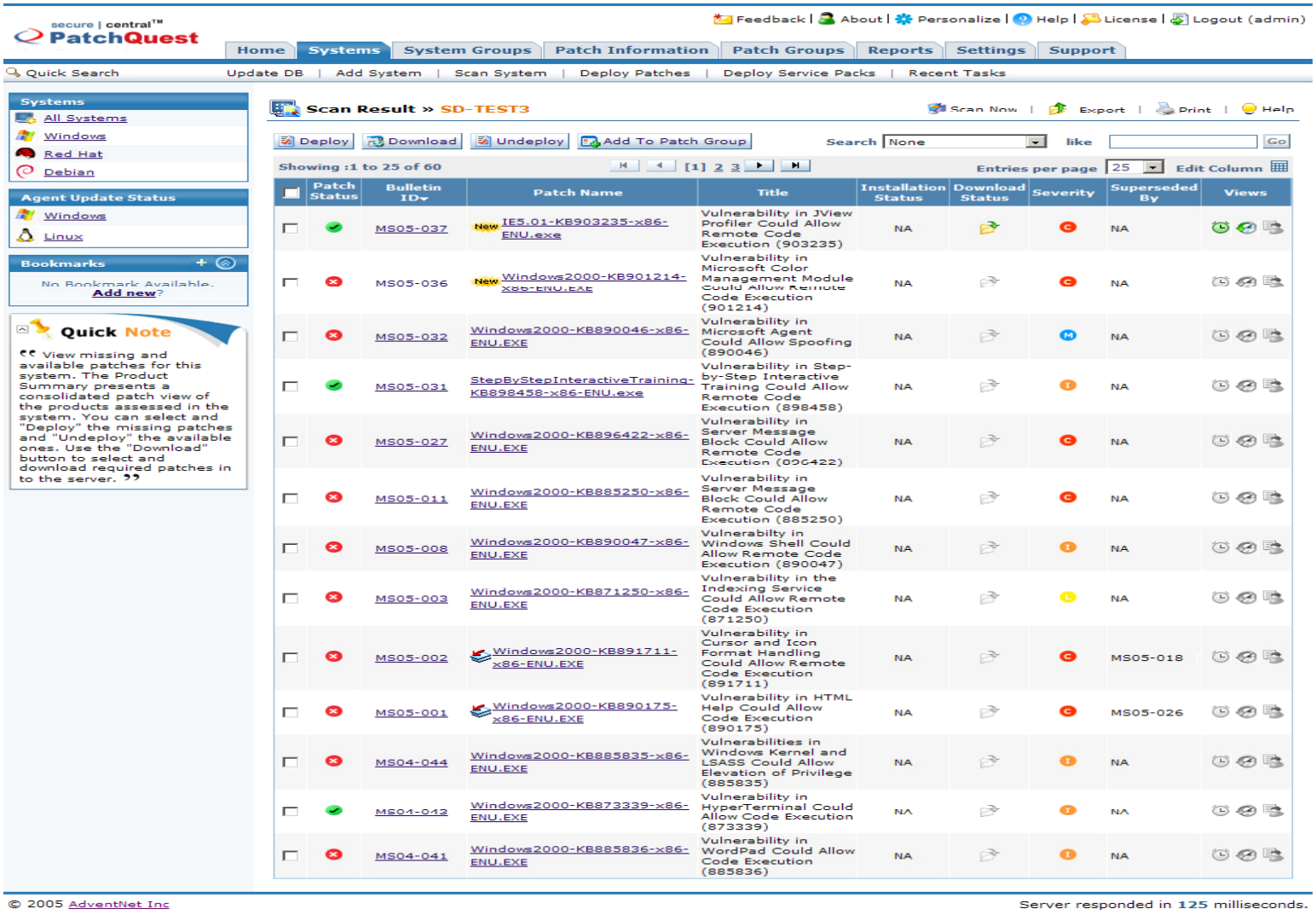
Features:

- Flexible modes of operation
- Web-based administration console for universal secure-access to data views and configurations
- Cross-platform product installation
- Array of reports to facilitate quick access to the data required

SecureCentral PatchQuest: Screenshot 1



SecureCentral PatchQuest: Screenshot 2



Tool: Patch Authority Ultimate

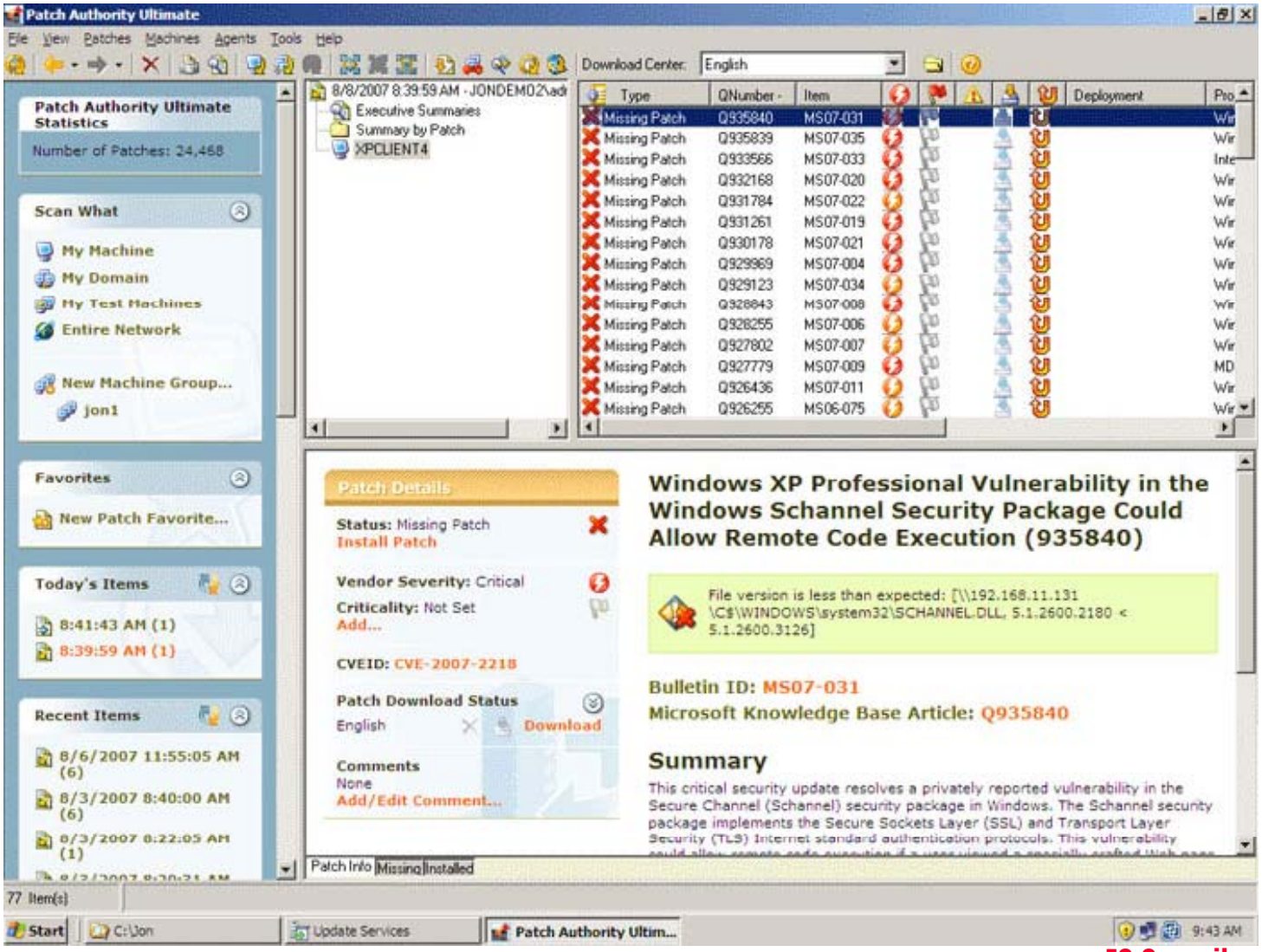
Patch authority ultimate is ScriptLogic's comprehensive and enterprise-class patch management solution

It prevents attacks and exploits through centralized control of updates on all Windows desktops and servers

Benefits:

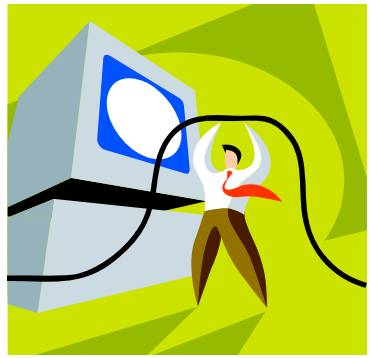
- Leading patch database and scan engine
- Selection, distribution, deployment, and reporting are all part of this comprehensive solution
- Management reports show overall patch status across the network
- Centralized management of patch policy and status for all computers, local and remote, on the LAN and across the Internet
- A baseline of patches can be created to establish a "secure" machine
- Enhanced security with central management of service status, configuration, logon accounts, and scheduled task configuration

Patch Authority Ultimate: Screenshot



Tool: ZENworks Patch Management

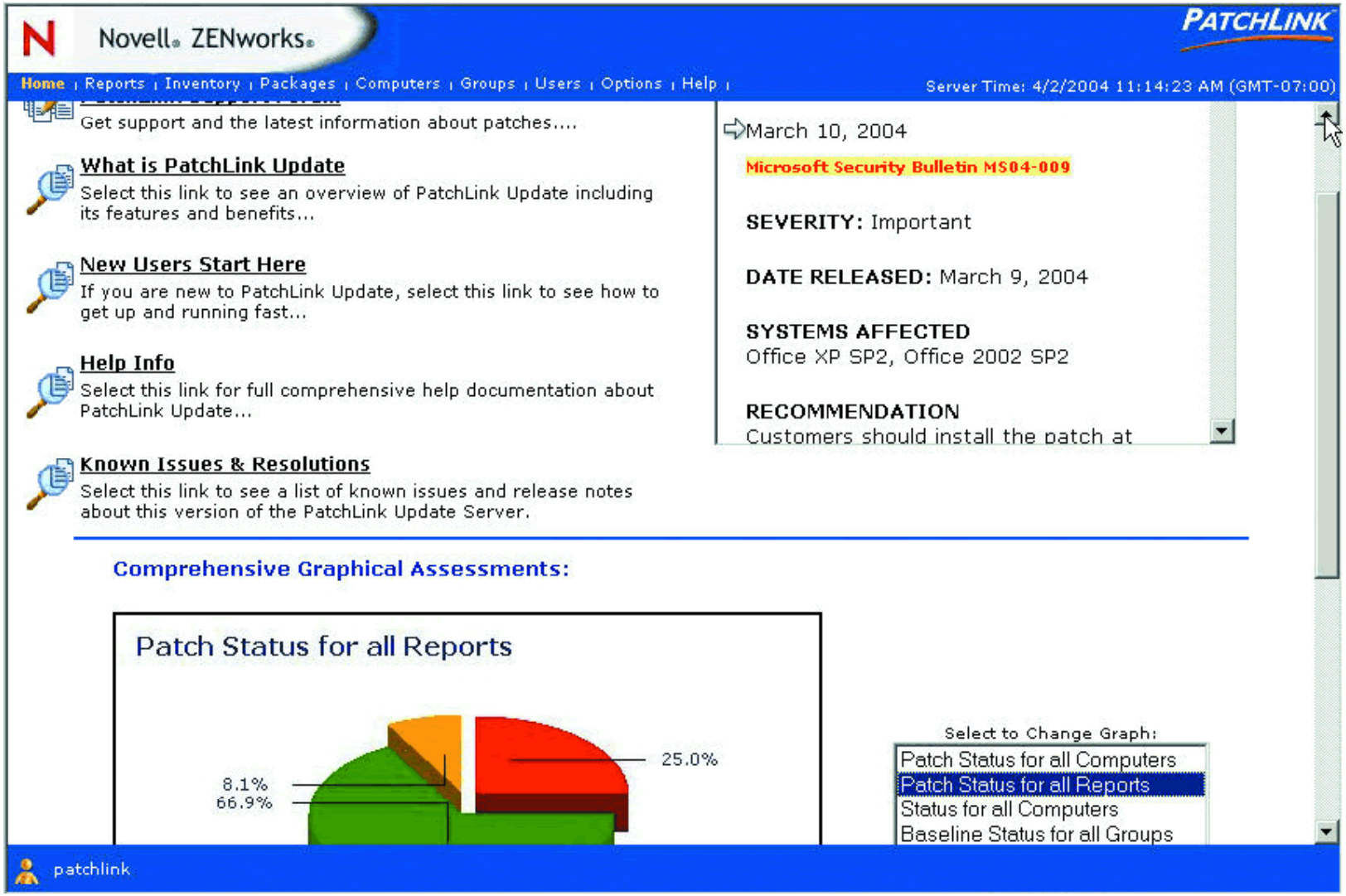
ZENworks Patch Management is a piece of automated patch management software



It can be used to protect your network from the viruses by automating the process of discovering security alerts, retrieving the patches, and deploying the right ones to the right machines at the right time to prevent problems

It provides patches for more than 40 different operating systems, applications, and software

ZENworks Patch Management: Screenshot



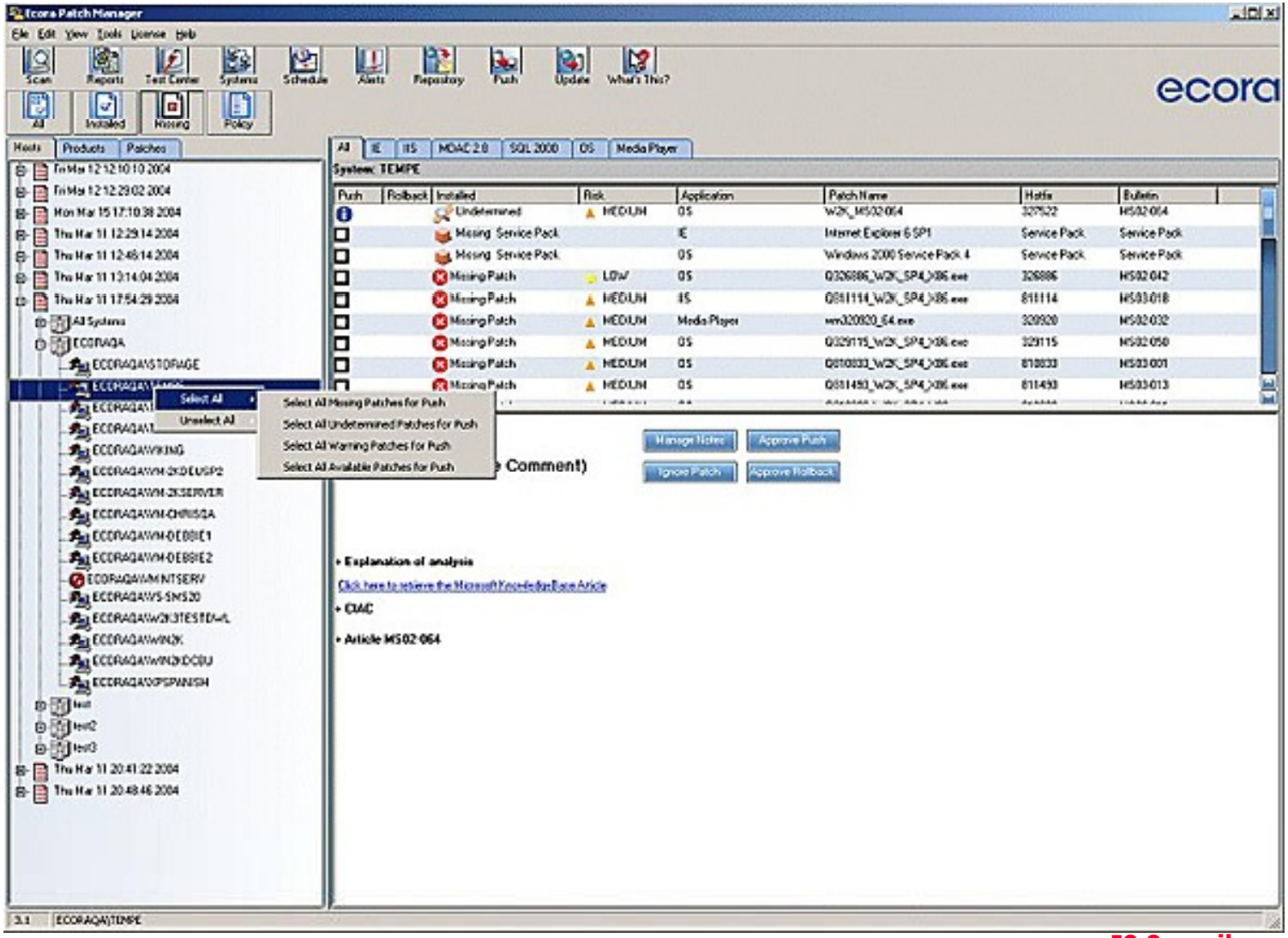
Tool: Ecora Patch Manager

Eroca Patch Manager automates system discovery, patch assessment, and patch installation on workstations and servers

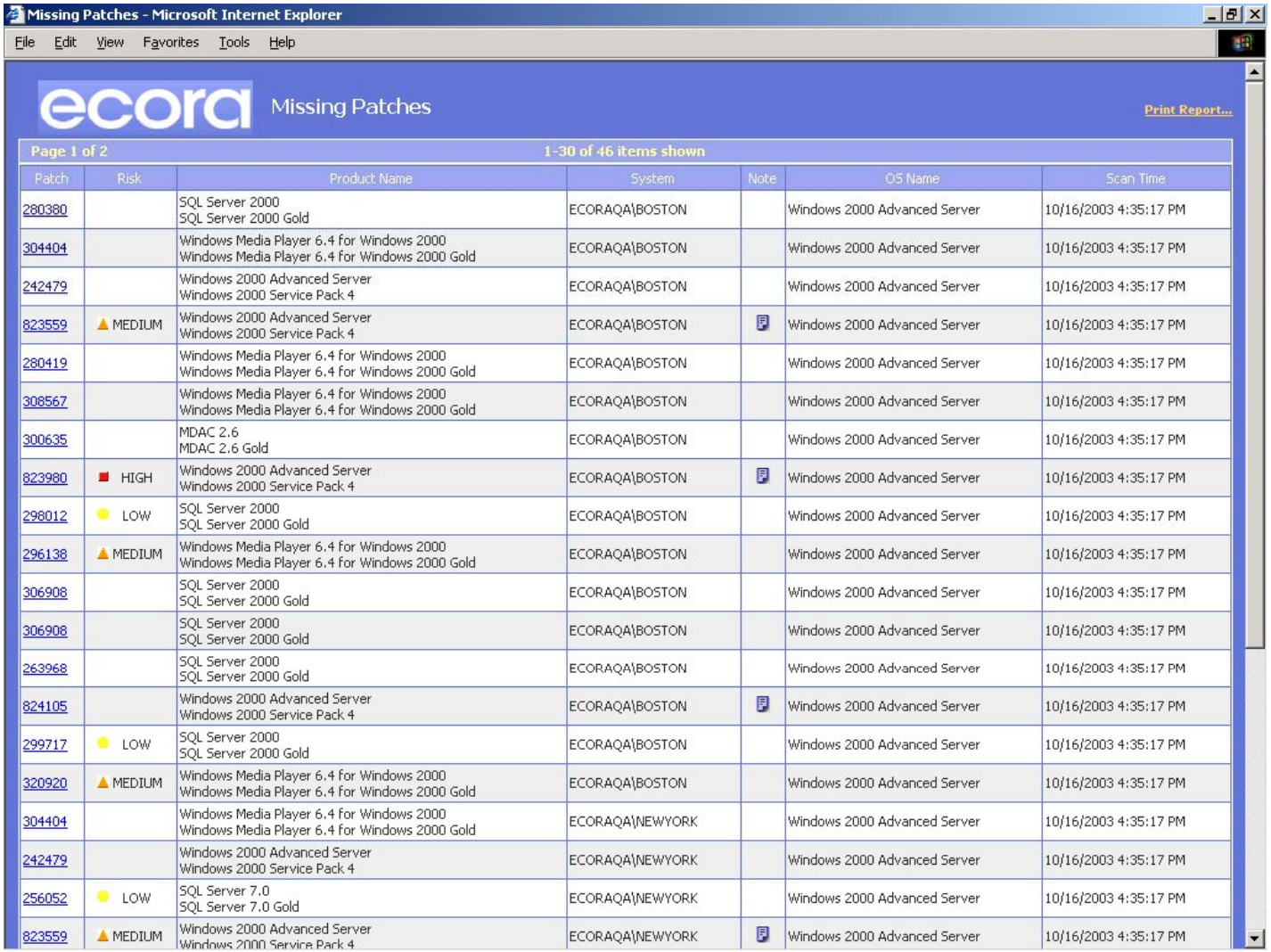
Features:

- Agent-less or optionally agent-based
- Views missing patches by systems, applications, specific patches, or according to your policy
- Patches any Windows application Microsoft supports, other companies' Windows-based patches, or patches for home grown applications
- Has automated patch roll-back on one or more machines
- Logically groups systems for ease of management
- Scheduled patch deployment

Ecora Patch Manager: Screenshot 1



Ecora Patch Manager: Screenshot 2



Patch	Risk	Product Name	System	Note	OS Name	Scan Time
280380		SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
304404		Windows Media Player 6.4 for Windows 2000 Windows Media Player 6.4 for Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
242479		Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
823559	MEDIUM	Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
280419		Windows Media Player 6.4 for Windows 2000 Windows Media Player 6.4 for Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
308567		Windows Media Player 6.4 for Windows 2000 Windows Media Player 6.4 for Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
300635		MDAC 2.6 MDAC 2.6 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
823980	HIGH	Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
298012	LOW	SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
296138	MEDIUM	Windows Media Player 6.4 for Windows 2000 Windows Media Player 6.4 for Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
306908		SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
306908		SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
263968		SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
824105		Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
299717	LOW	SQL Server 2000 SQL Server 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
320920	MEDIUM	Windows Media Player 6.4 for Windows 2000 Windows Media Player 6.4 for Windows 2000 Gold	ECORAQA\BOSTON		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
304404		Windows Media Player 6.4 for Windows 2000 Windows Media Player 6.4 for Windows 2000 Gold	ECORAQA\NEWYORK		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
242479		Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\NEWYORK		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
256052	LOW	SQL Server 7.0 SQL Server 7.0 Gold	ECORAQA\NEWYORK		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM
823559	MEDIUM	Windows 2000 Advanced Server Windows 2000 Service Pack 4	ECORAQA\NEWYORK		Windows 2000 Advanced Server	10/16/2003 4:35:17 PM

Tool: Service Pack Manager

Service Pack Manager enables system administrators to fix security vulnerabilities and stability problems in Windows NT/2000/XP/2003 and additional Microsoft products

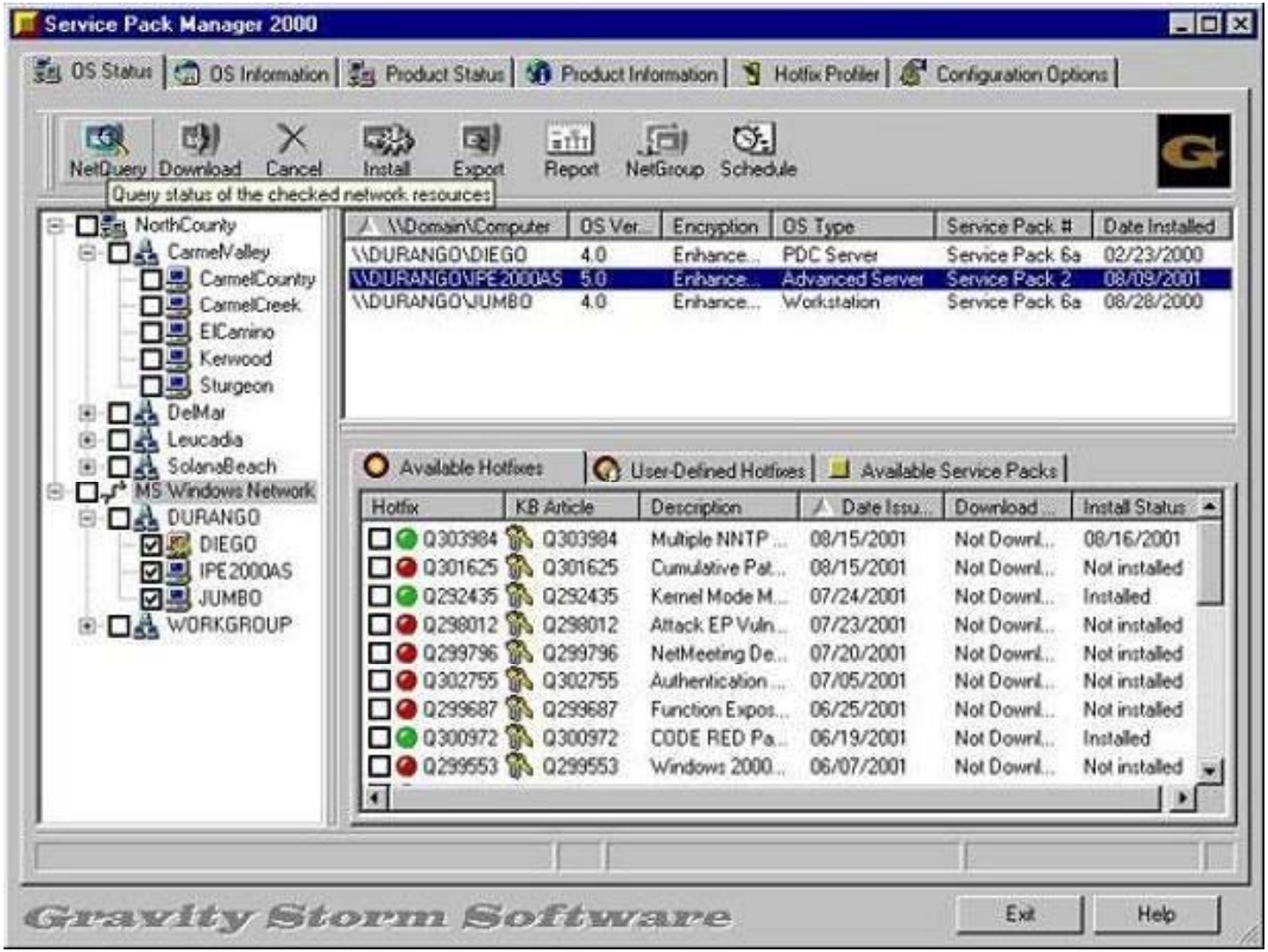
It allows to remotely detect, track, monitor, and install Windows NT/2000/XP/2003 Service Packs and Hotfixes on the enterprise networks from a central console

Remote inventory, research, and deployment of the security vulnerabilities patches and stability updates make Service Pack Manager a highly cost-effective tool when used on the enterprise LANs and WANs

The installation status of hundreds of hotfixes can be detected quickly on any number of remote computers

It makes the task of maintaining security of the large networks viable

Service Pack Manager: Screenshot



Tool: Altiris Patch Management Solution

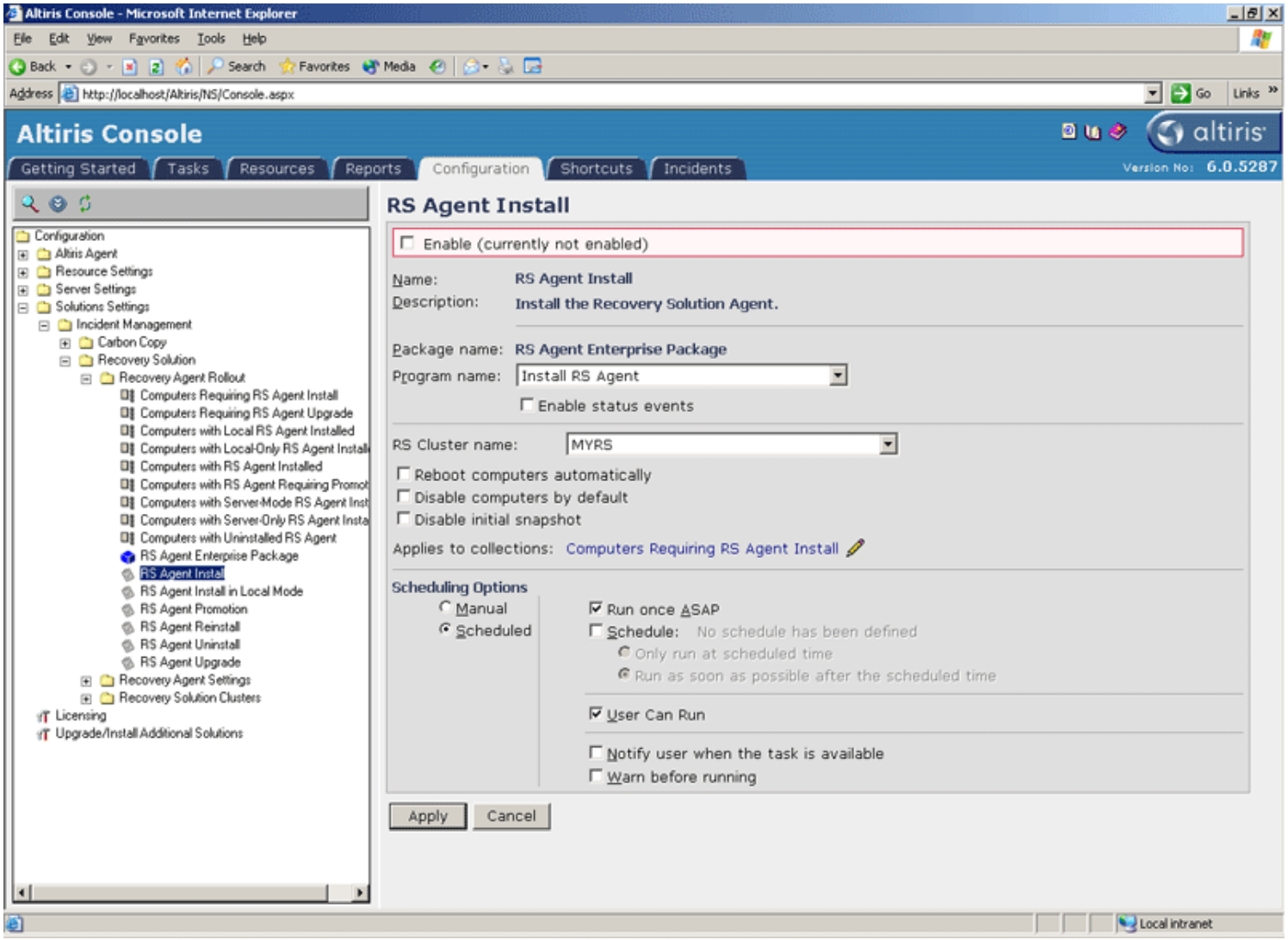
Altiris Patch Management Solution software proactively manages patches and software updates by automating the collection, analysis, and delivery of patches across your enterprise

It helps you to decrease the costs involved in delivering patches throughout your enterprise and integrates with Altiris Recovery Solution for stable-state rollback

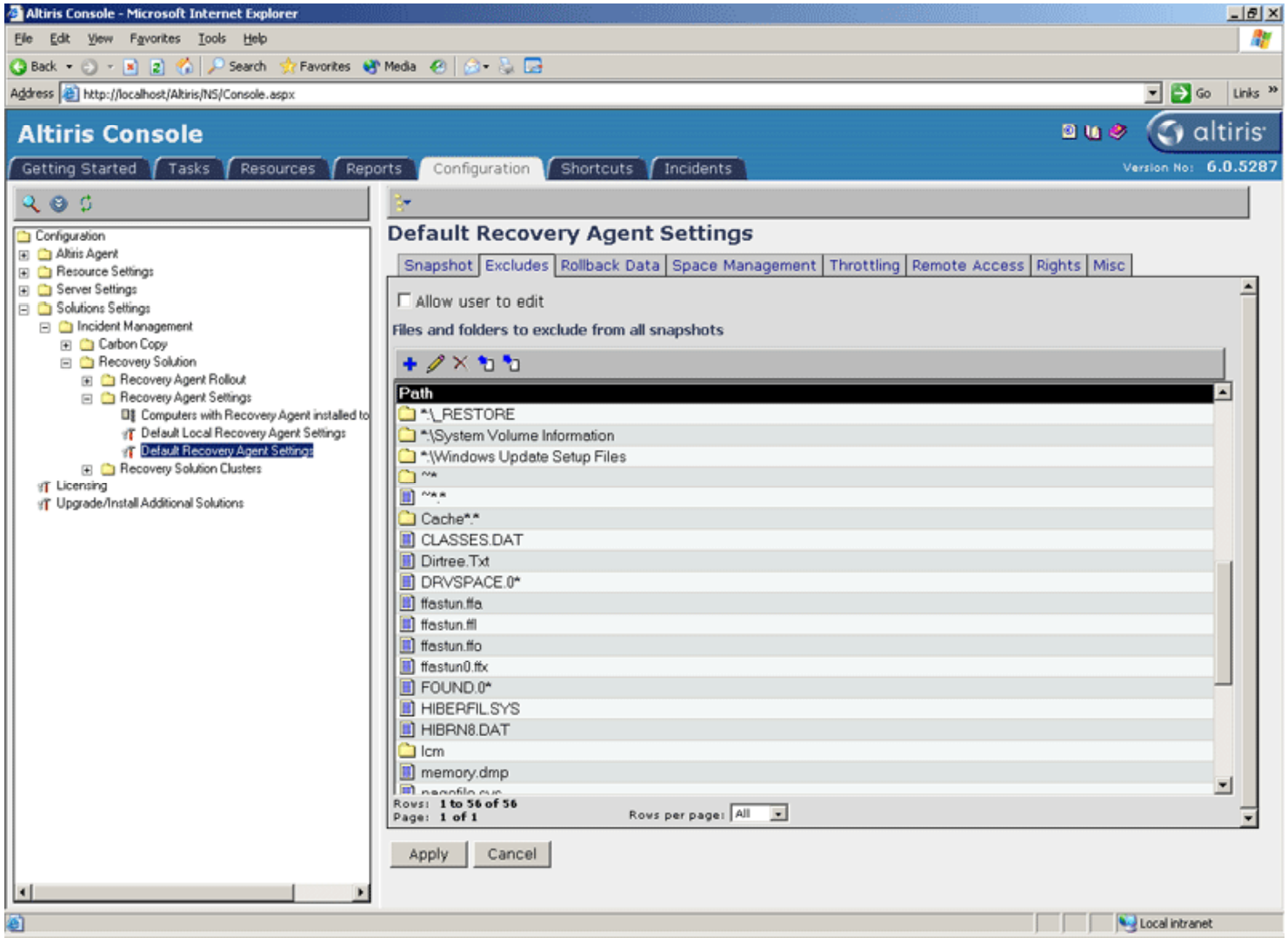
It provides improved functionality in the analysis, collection, and distribution of OS and application updates

It improves business continuity and accelerates IT systems' security by reducing the need for extended patch test cycles

Altiris Patch Management Solution: Screenshot 1



Altiris Patch Management Solution: Screenshot 2



Tool: BMC Patch Manager

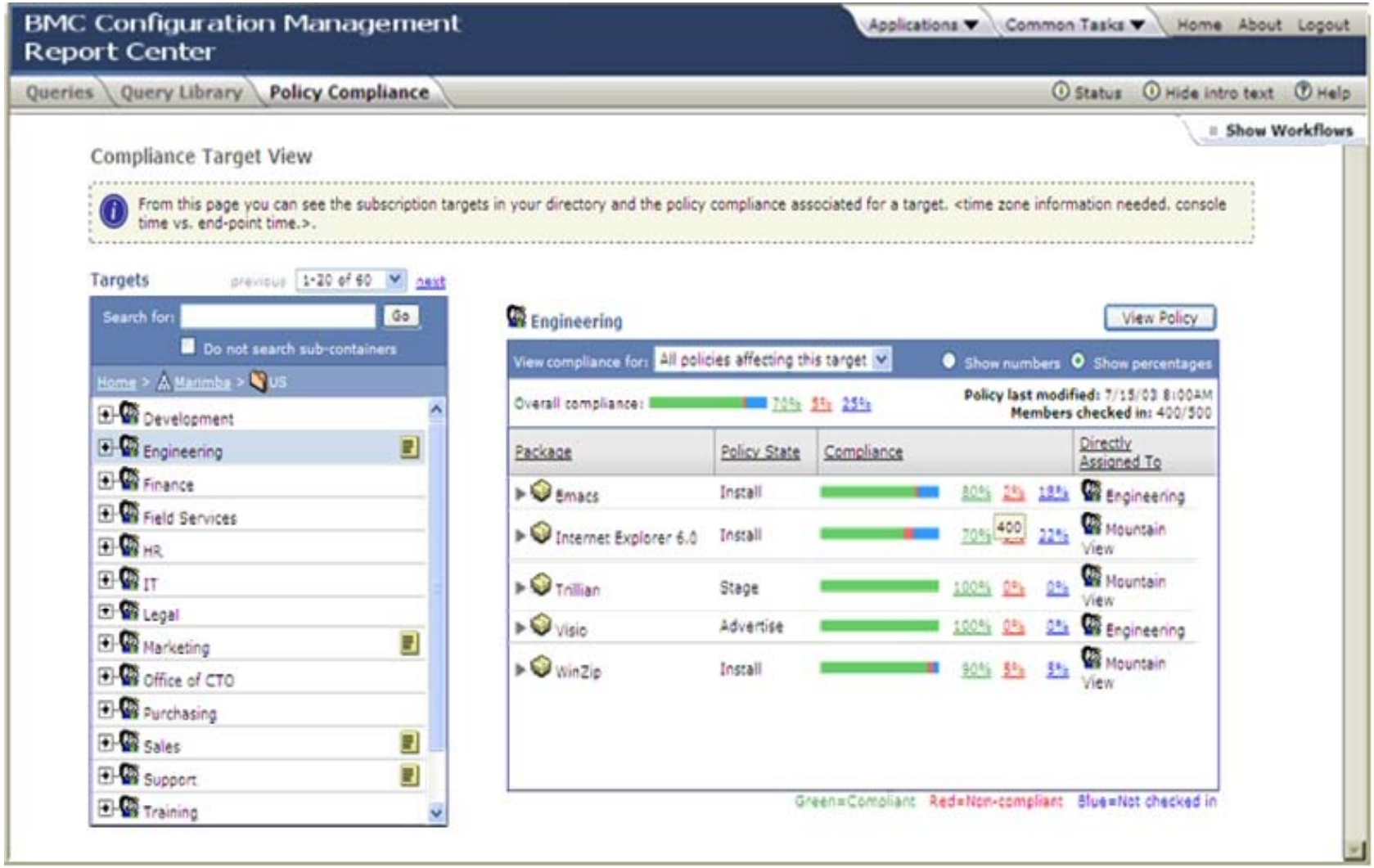
BMC Patch Manager enables you to manage and deploy security and functional patches on desktops, laptops, PDAs, and servers

By automating critical patch management functions (patch collection, preparation, testing, staging, deployment, auditing), it helps you to save time, improve response times, and reduce attack-related risks

Features:

- Provides patch-testing capabilities that allow administrators to group test patch installations within sample environments
- Allows you to deploy patches based on security policies for ongoing operations or specific tasks for emergency deployments
- Identifies vulnerabilities, automatically delivers critical patches, and fixes to thousands of endpoints, and verifies deployment success
- Allows you to proactively manage the distribution of patches including functional, anti-virus, and security patches to lower patch management costs

BMC Patch Manager: Screenshot



Tool: Hotfix Reporter

Hotfix Reporter is a tool that works in conjunction with the Microsoft Network Security Hotfix Checker (HfNetChk) tool to scan your network server for missing patches

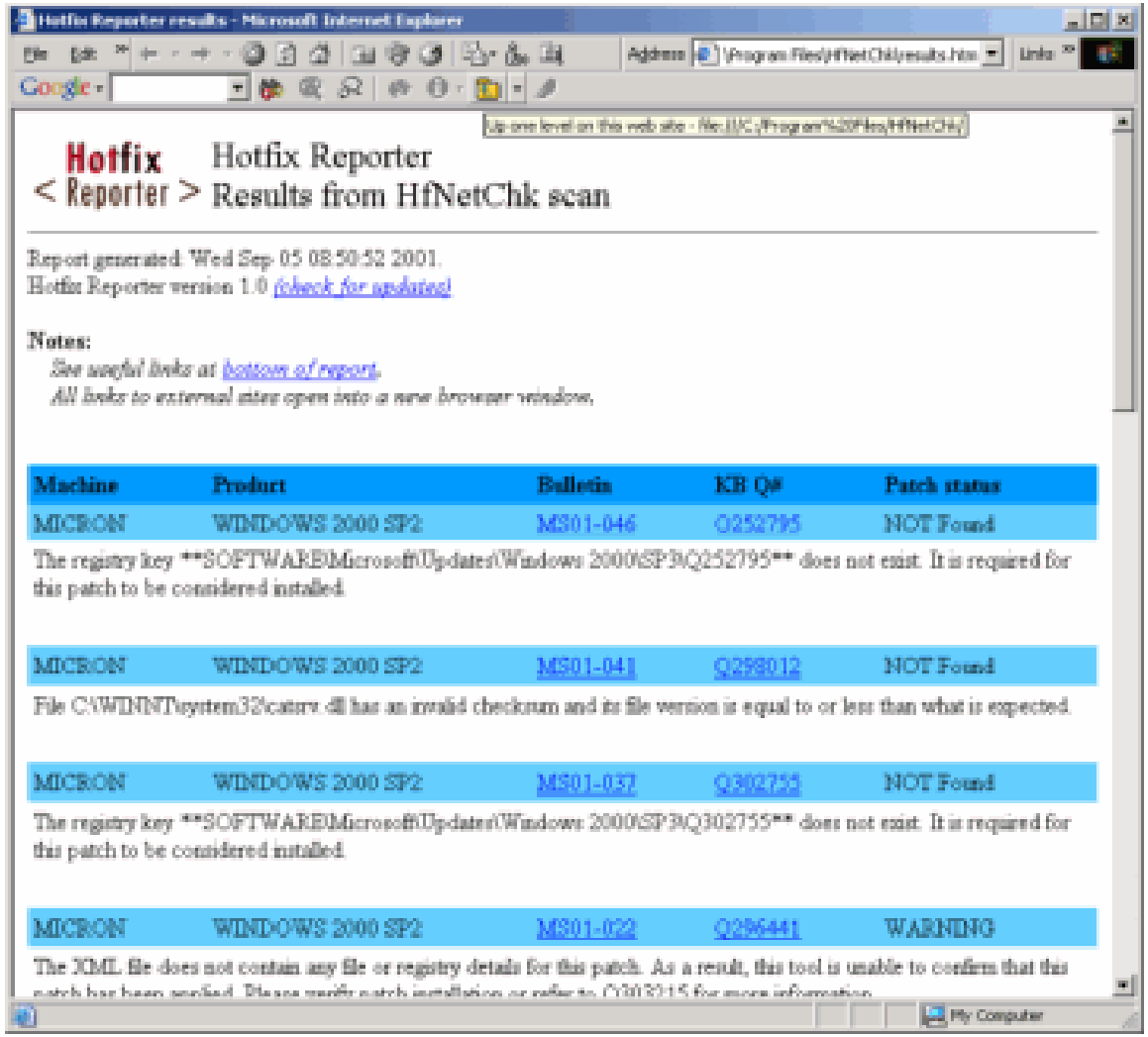
HfNetChk scans your system for missing patches, but displays the results in a raw, plain-text, and unfriendly format

Hotfix Reporter converts the HfNetChk's raw output into an HTML page, complete with clickable links, making it easy to download the necessary patches from Microsoft

Features:

- Converts HfNetChk output into user-friendly HTML
- Tells you if the scan gave different results than the last time it was run, making it easy to quickly tell if any new patches have been released
- Displays Microsoft security bulletin numbers and knowledgebase article numbers as clickable links
- Shows the most recent patches first

Hotfix Reporter: Screenshot



Hotfix Reporter results - Microsoft Internet Explorer

Hotfix Reporter

Hotfix Reporter
Results from HfNetChk scan

Report generated: Wed Sep 05 08:50:52 2001.
Hotfix Reporter version 1.0 (check for updates)

Notes:

See useful links at bottom of report.
All links to external sites open into a new browser window.

Machine	Product	Bulletin	KB Q#	Patch status
MICRON	WINDOWS 2000 SP2	MS01-046	Q252795	NOT Found
The registry key **SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q252795** does not exist. It is required for this patch to be considered installed.				
MICRON	WINDOWS 2000 SP2	MS01-041	Q298012	NOT Found
File C:\WINNT\system32\catsrv.dll has an invalid checksum and its file version is equal to or less than what is expected.				
MICRON	WINDOWS 2000 SP2	MS01-037	Q302755	NOT Found
The registry key **SOFTWARE\Microsoft\Updates\Windows 2000\SP3\Q302755** does not exist. It is required for this patch to be considered installed.				
MICRON	WINDOWS 2000 SP2	MS01-022	Q296441	WARNING
The XML file does not contain any file or registry details for this patch. As a result, this tool is unable to confirm that this				

Tool: Numara Patch Manager

Numara Patch Manager is a tool used to update and download patches for Microsoft's operating systems and applications across your entire network

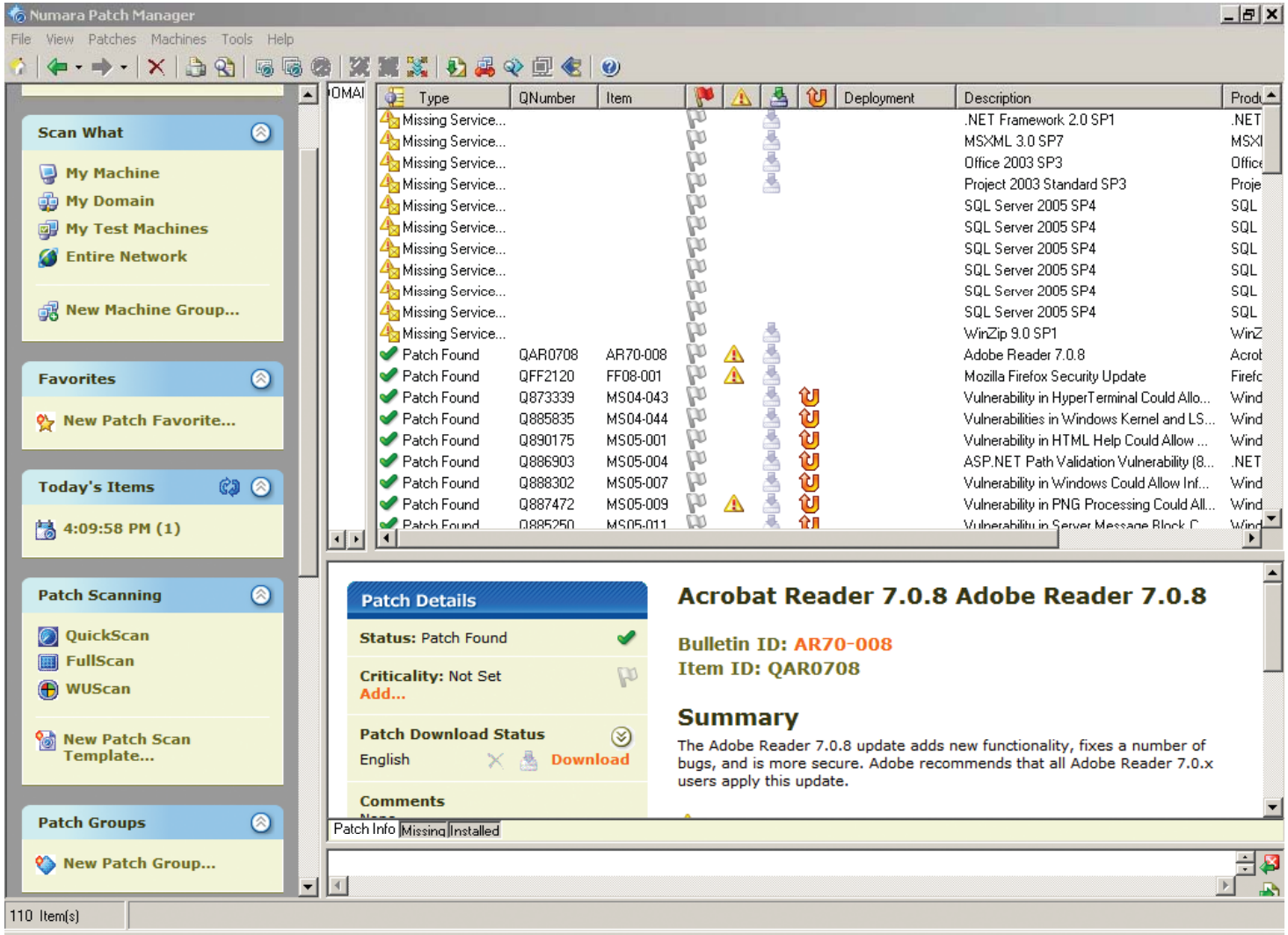
It allows you to assess the patch status of all Microsoft-based workstations as well as validate any existing patches that have been installed

It create baseline patch groups and scan groups of workstations to determine which ones are compliant and which ones are not

It can also be used to perform patch scans during non-business hours or off-peak bandwidth periods

Administrators can reboot workstations immediately or at a specified date or time

Numara Patch Manager: Screenshot



Tool: TrueUpdate

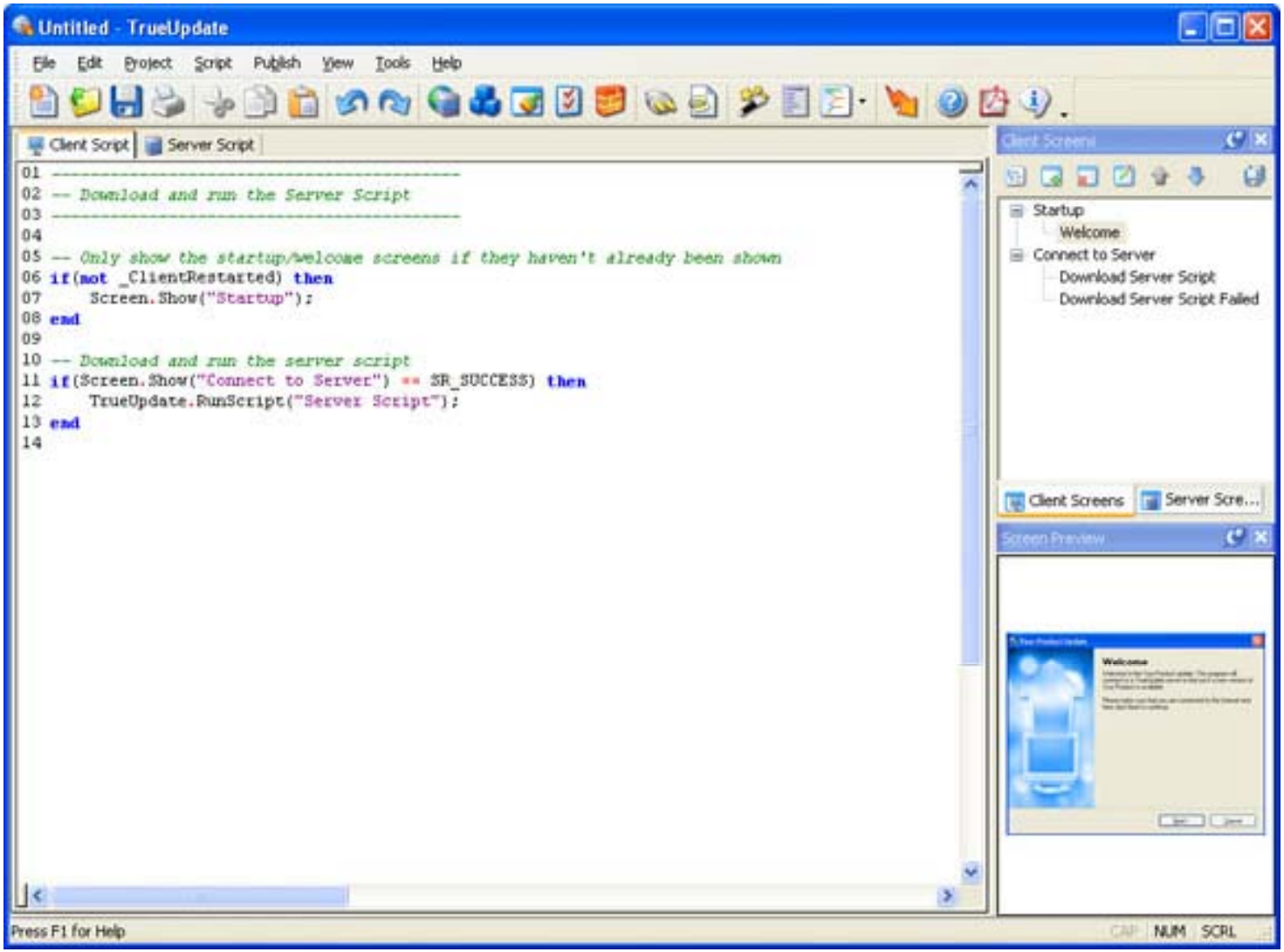
TrueUpdate is a comprehensive solution for software developers wanting to integrate automatic updating capabilities into their software applications

It gives you a robust client/server framework for determining required updates, and then retrieving and applying the necessary patches or installation files using standard Internet protocols

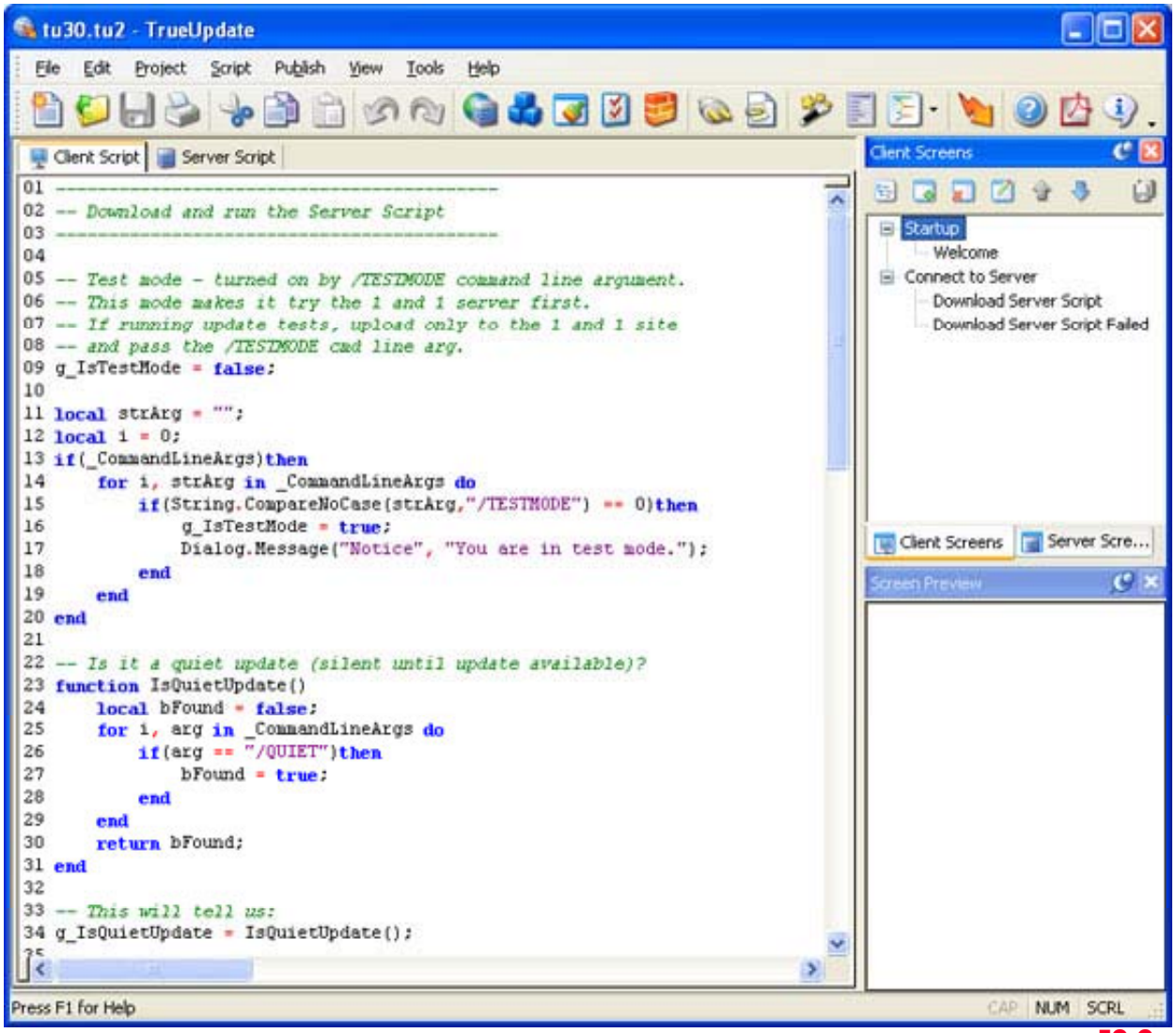
Features:

- The client can easily be integrated into existing software or installed as a standalone application
- Compatible with any update/patching method, from full setups and self-contained binary patches to download and extract from zip files
- The system is always up-to-date with the latest software and patches
- Includes more than 250 high level actions with everything from registry editing and file copying to web server script interaction and much more

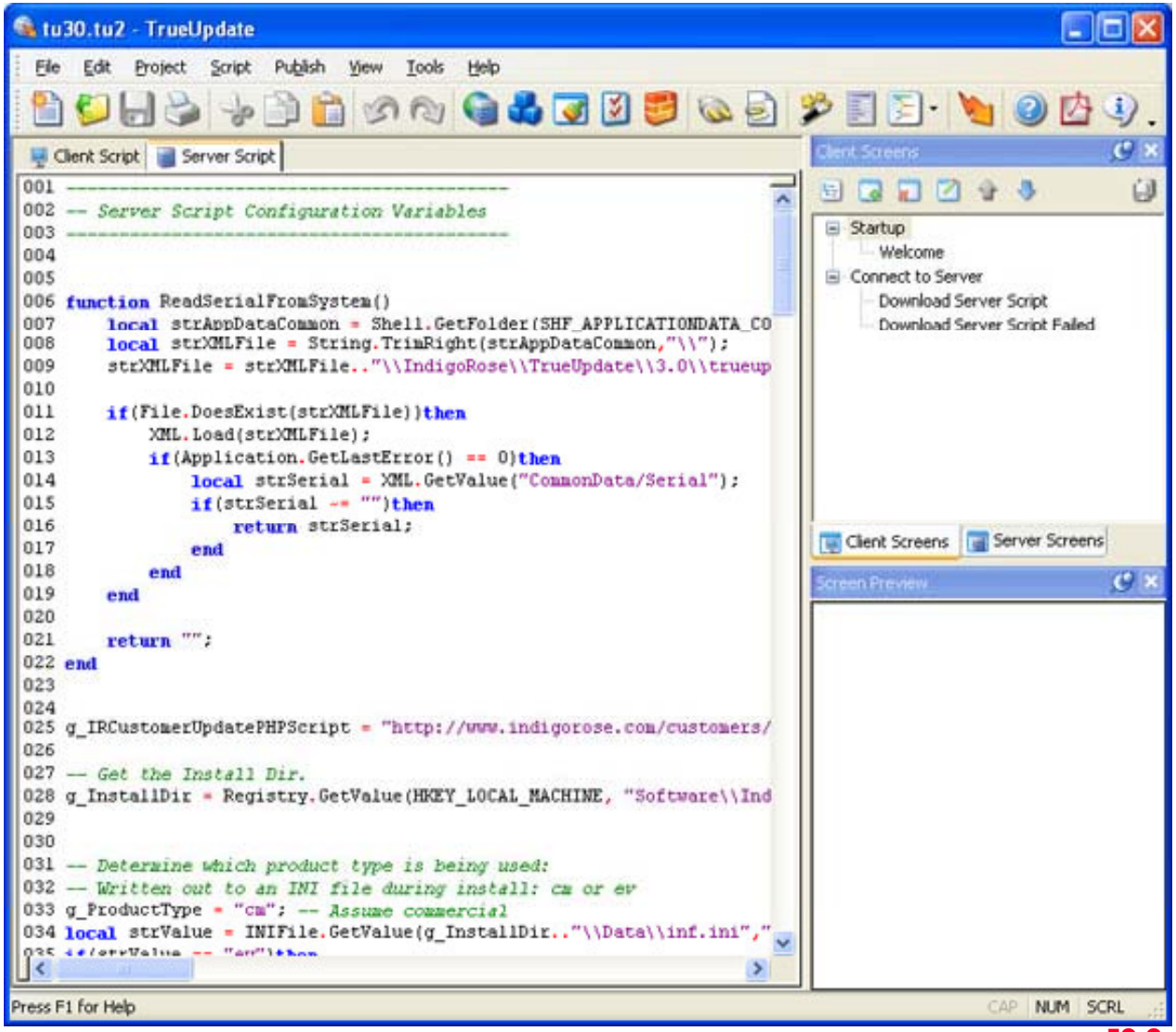
TrueUpdate: Screenshot 1



TrueUpdate: Screenshot 2



TrueUpdate: Screenshot 3



Tool: FlashUpdate

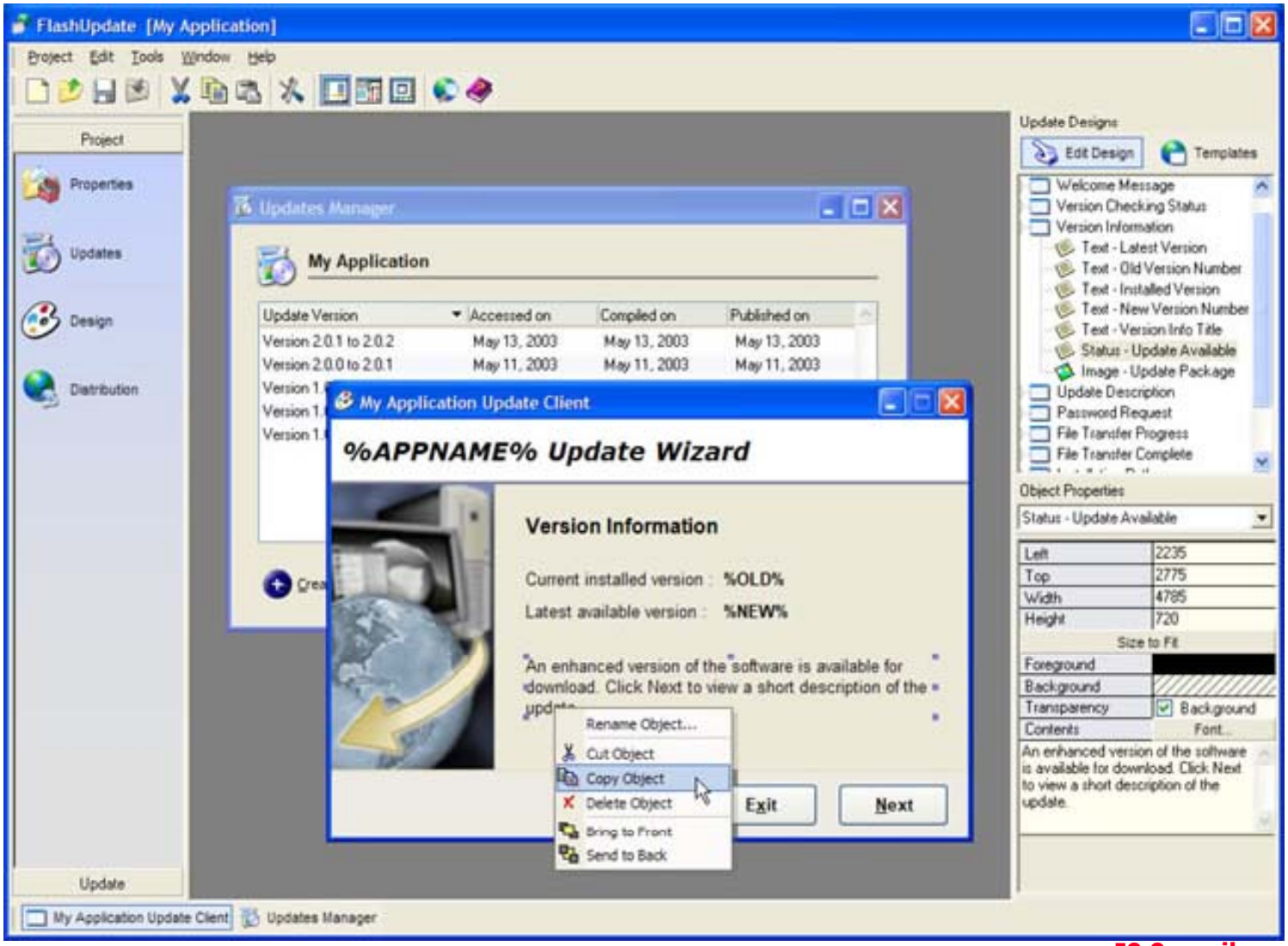
FlashUpdate is a software update solution for windows developers

It allows you to create, manage, and distribute your software updates and patches in a flash

Features:

- Advanced Patch Engine provides up to 98% file compression
- Adaptive patch creation for optimal patch size and speed efficiency
- Support for all file types, including executable files, system files, data files, and documents
- Native support for shared and locked files
- Helps to prevent software piracy

FlashUpdate: Screenshot



Tool: Microsoft Software Update Services (SUS)

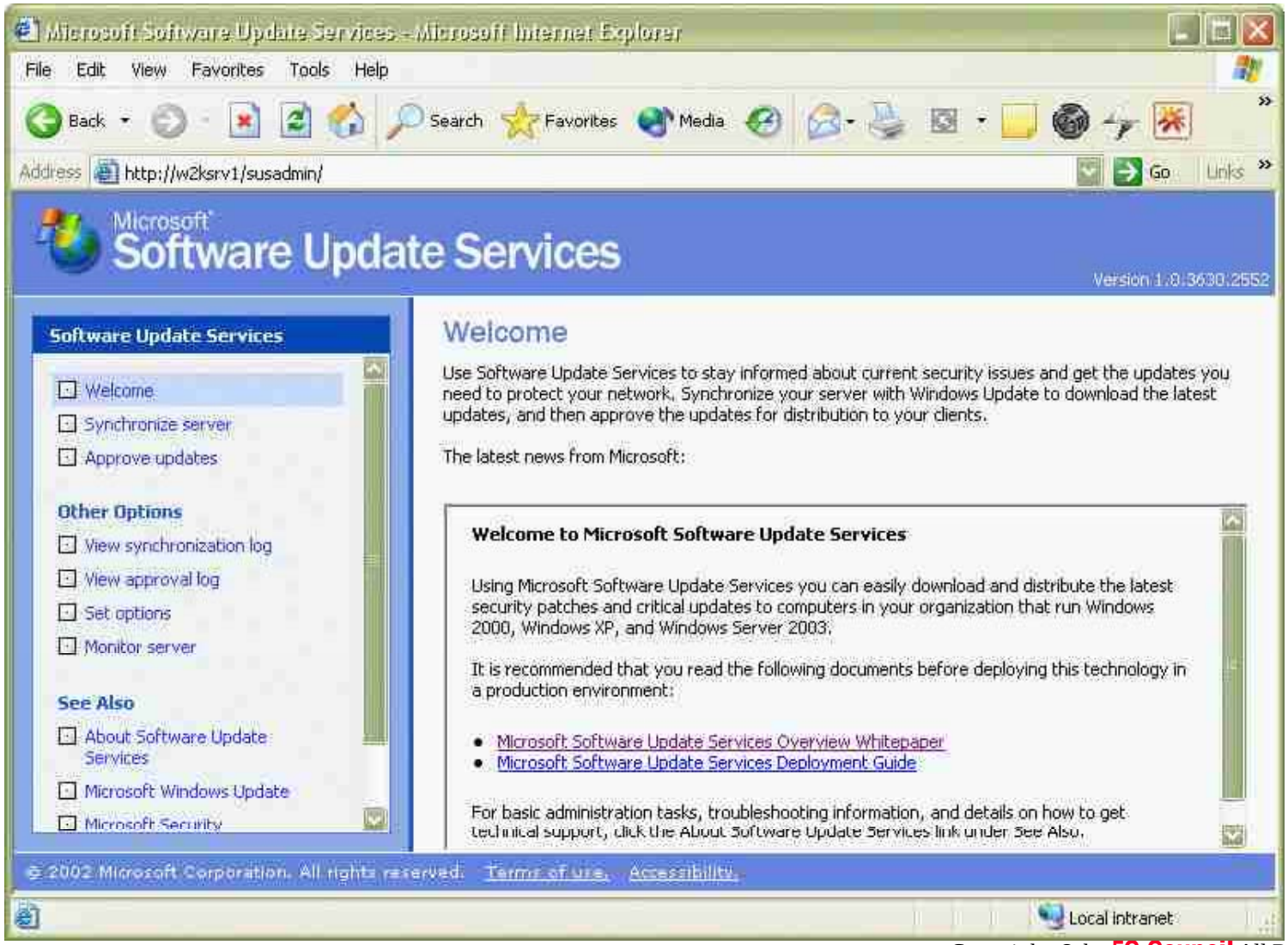
Software Update Services (SUS) supports updating for a broader set of Microsoft products and provides robust management and reporting features

It connects through your firewall to the windows update site and allows IT administrators to import critical updates, security updates, and service packs

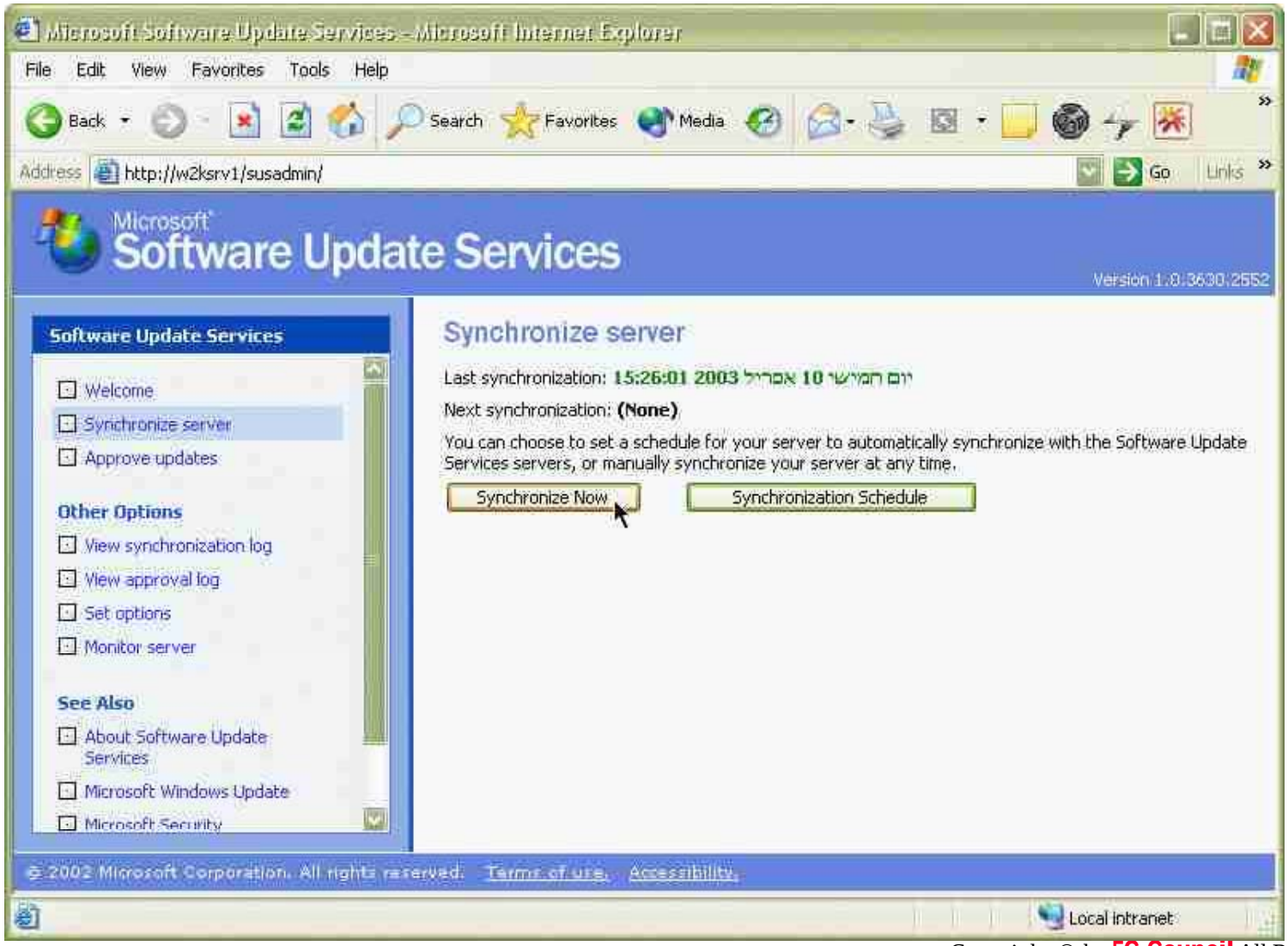
Administrators can receive e-mail notification when updates are added to their SUS pipeline

It consists of both client-side and server-side components to provide a basic solution to critical update management

Microsoft Software Update Services (SUS): Screenshot 1



Microsoft Software Update Services (SUS): Screenshot 2



Tool: Prism Patch Manager

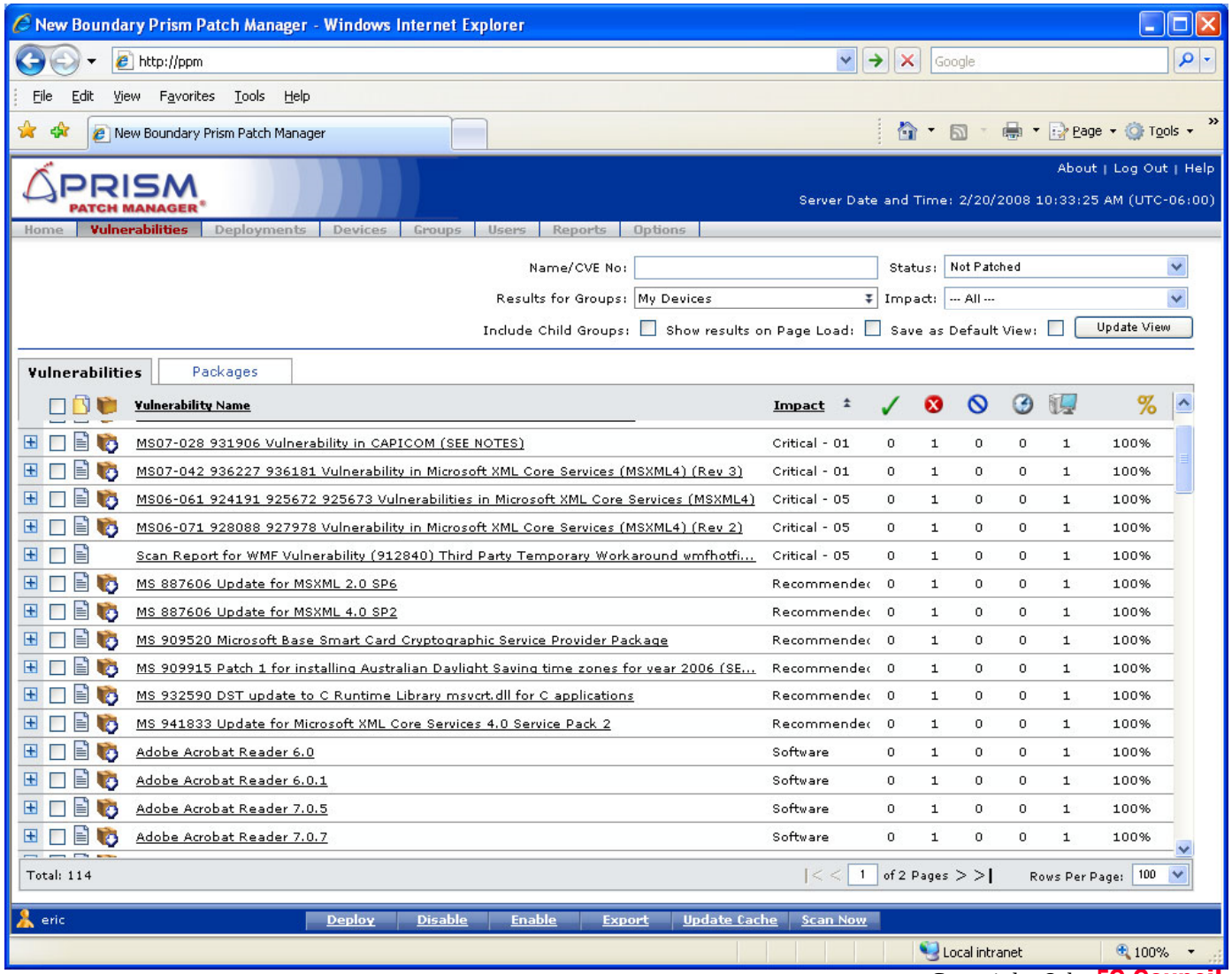
Prism Patch Manager automatically secures windows systems from software vulnerabilities by managing the entire software patching process

It manages the software patching process such as discovering vulnerabilities, acquiring and testing patches, and deploying patches

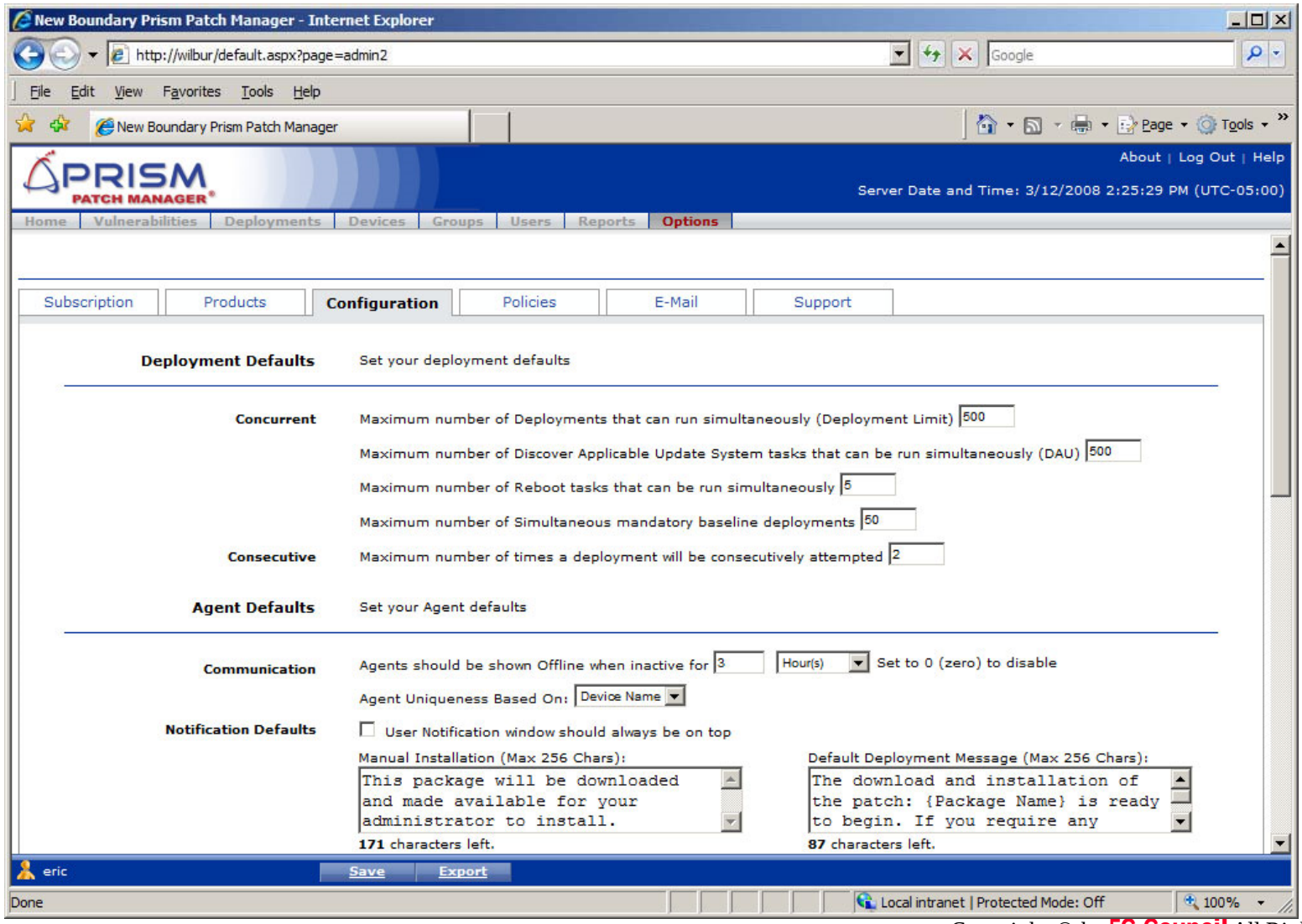
It delivers comprehensive reporting to demonstrate patch compliance to management and auditors

It reduces organizational risk, improves IT productivity, and lowers the cost of IT infrastructure maintenance

Prism Patch Manager: Screenshot 1



Prism Patch Manager: Screenshot 2



Tool: Patch-Magic

Patch-Magic updates all computer systems in your network

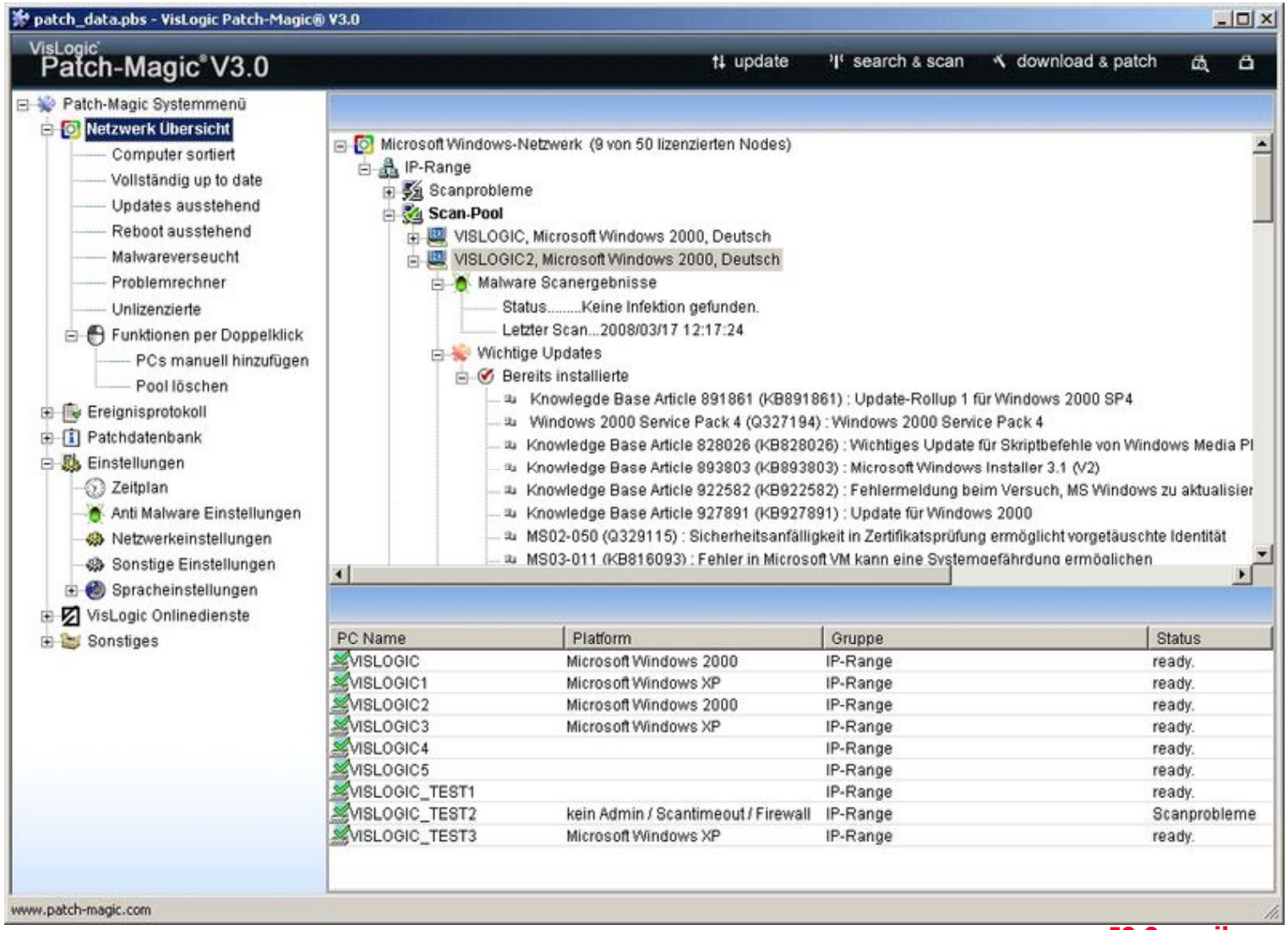
It avoids viruses and worms, and minimizes security risks

It can be used to scan each system individually, to discover necessary patches and updates, and to install them remotely

Features:

- Intuitive view and description of missing patches
- Automates patch download and individual deployment
- Identifies and removes remote malware in your LAN
- Time scheduler for scans, deployment, and data base update
- Supports virus scanning proxy servers / firewalls
- Centralized storage of patches at the location of your choice (patch library)
- Intelligent reboot handling

Patch-Magic: Screenshot



Patch Management Checklist

How often and when do you apply patches?

Who can deploy and/or authorize updates?

How are patches tested prior to rollout?

What problems will trigger a rollback?

Best Practices for Patch Management

- Test the patch before rollout to ensure that the applied patch is compatible with other applications
- You need to have a rollback version when the applied patch fails
- Do not deploy multiple patches simultaneously across the network as it will halt other applications and will be inconvenient for users
- Deploy the patches after production hours as reboot is required for maximum patches
- Always check for latest releases to minimize downtime as often a user calls or virus initiates a frantic search for a missing patch
- If you patch regularly, you need to keep track of what fixes were applied, when, for auditing and reporting
- Follow the defined patch process which specifies who may approve patches and procedures to deploy them

Summary

- A hotfix is a code that fixes a bug in a product
- Patch Management is the process of correcting deficiencies and updating software with the latest features
- Windows patch management involves: testing, deployment, and validation
- Microsoft Software Update Services (SUS) hosts windows updates
- Designing a deployment plan to distribute patch on a timely basis is one of the best practices in the patch management