



Ethical Hacking and Countermeasures

Version 6

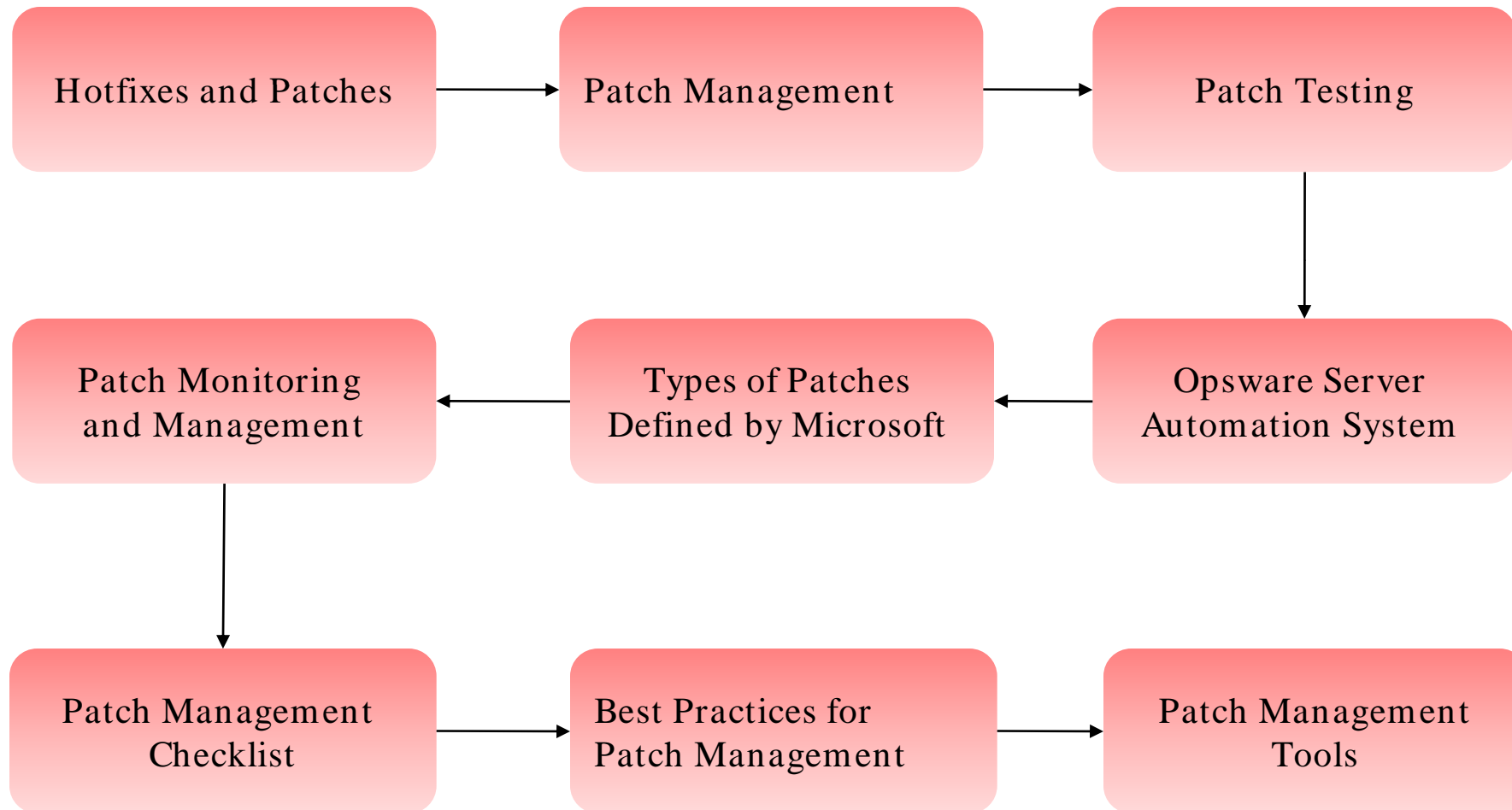


Module LXV

Patch Management

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



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

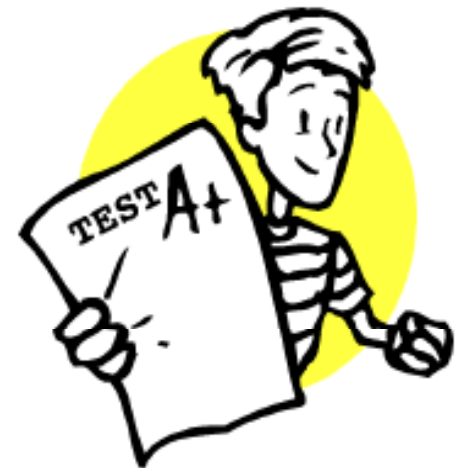
The first step in patch testing is the verification of patch source and integrity which helps you to ensure that update is valid and it is not altered

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

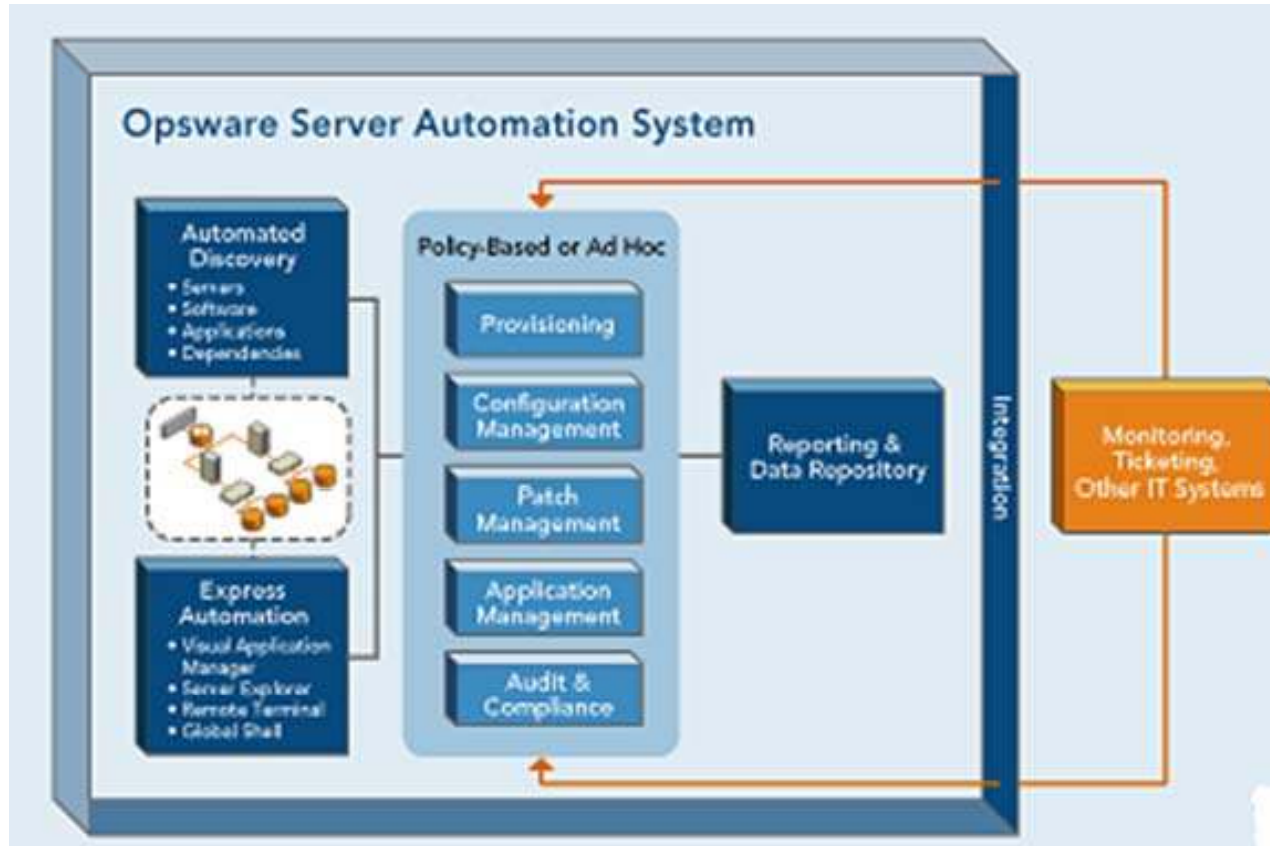
It gives administrators the ability to monitor systems and apply configuration changes across many servers in a uniform fashion

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

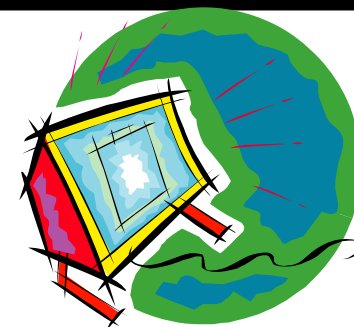
The administrator can then use Opsware to rollback the change or propagate the change throughout the server environment

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



Patch Management Tools

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

The screenshot shows the UpdateExpert application window. On the left, a tree view lists machines on the network 'RKAPLAN'. The main pane displays a 'Research View' table of updates. A 'Component Install Wizard' dialog box is open, showing the selected update 'Q265714.EXE' and installation options.

Name	KB Article	Reason for fix	Release Date	Install Date	Language
Q246988l.exe	Q246988	Default Gateway Is Ignored When IRDP Is Enabled	11/24/1999	Not installed	English
Q275713l.exe	Q275713	Access Violation When RAS Is Disabled	10/13/2000	Not installed	English
Q259728l.EXE	Q259728	Windows NT 4.0 Security Patch: IP Fragment Reassembly...	05/08/2000	11/10/2000	English
Q269239l.EXE	Q269239	Windows NT4 Security Patch: NetBIOS Name Server Prot...	08/18/2000	11/10/2000	English
Q243649l.EXE	Q243649	Windows NT 4.0 Security Patch: Microsoft Print Spooler S...	11/03/1999	11/10/2000	English
Q246954l.exe	Q246954	Unattended RAS Installation Prompts for New IP Address	11/24/1999	Not installed	English
Q262463l.EXE	Q262463	Find.exe Returns Extra Lines When Piped	05/09/2000	Not installed	English
Q283001l.exe	Q283001	Windows NT 4.0 Security Patch: Malformed PPTP Packet...	02/14/2001	Not installed	English
Q265714l.EXE	Q265714	Windows NT 4.0 Security Patch: SNMP Parameters Vulne...	12/22/2000	Not installed	English

Component Install Wizard
 Install Components
 Customize the install time and options.

Machines Selected: RKAPLAN
 HotFix Selected: Q265714l.EXE
 Installed Time: 04/27/2001 05:00PM

Install Now

Options:

- Do not create uninstall...
- Force apps to close on...
- Quiet mode
- Reboot after each install
- Reboot after group inst...

Buttons: Done, Cancel

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

```
C:\WINNT\System32\cmd.exe
MICRON
-----
WINDOWS 2000 SP2
Patch NOT Found MS00-077      Q299796
Patch NOT Found MS00-079      Q276471
Patch NOT Found MS01-007      Q285851
Patch NOT Found MS01-013      Q285156
WARNING          MS01-022      Q296441
Patch NOT Found MS01-025      Q296185
Patch NOT Found MS01-037      Q302755
Patch NOT Found MS01-041      Q298012

Internet Information Services 5.0
Patch NOT Found MS01-025      Q296185

Internet Explorer 5.5 SP2

INFORMATION
All necessary hotfixes have been applied
```


caccls.exe Utility

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

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

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



```
Command Prompt
C:\Snort>caccls.exe *.exe /T /G System:F Administrators:F
Are you sure (Y/N)?y
processed file: C:\Snort\snort.exe
C:\Snort>
```

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

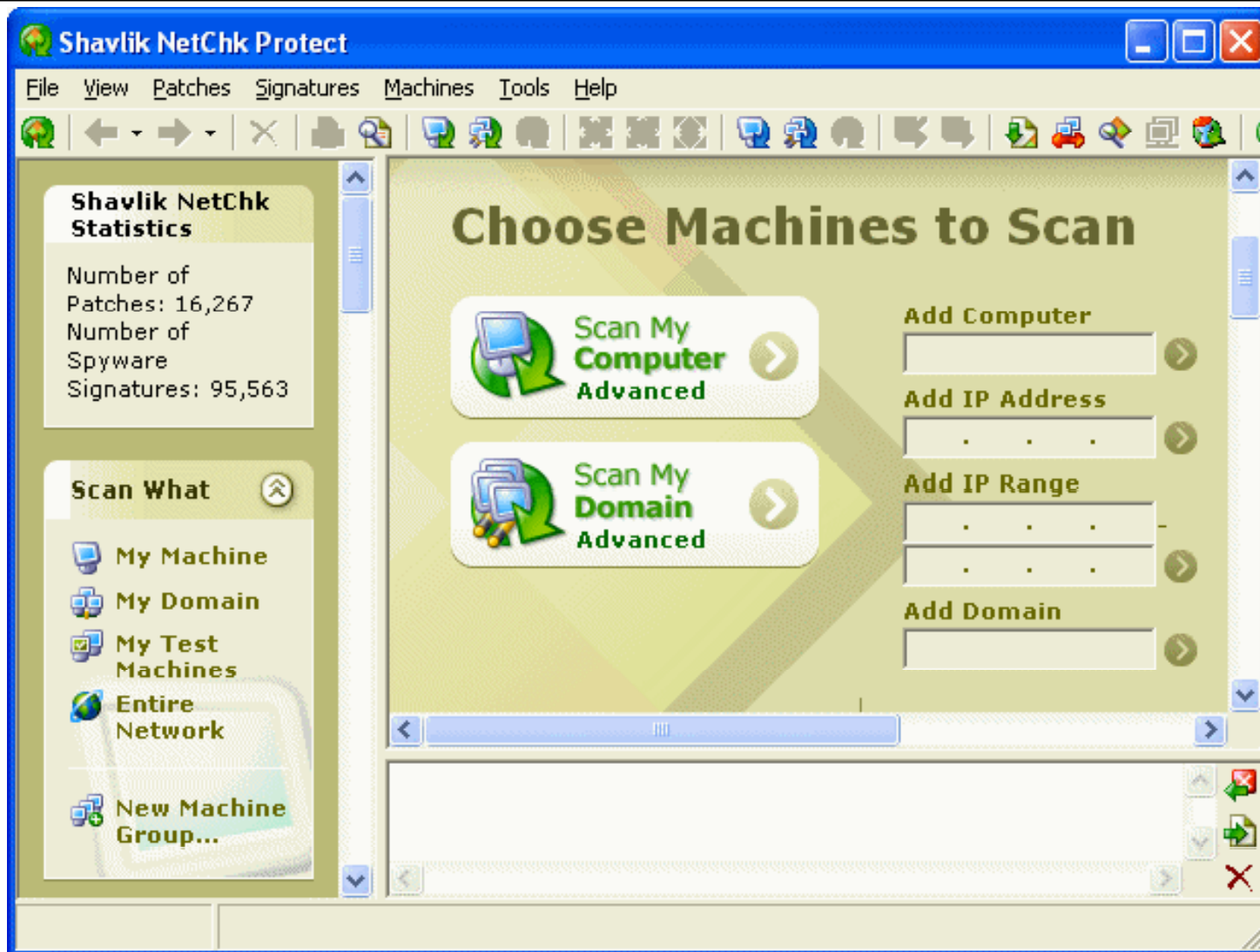
It offers a solution for detecting, removing, and managing critical threats and vulnerabilities with active vulnerability management

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

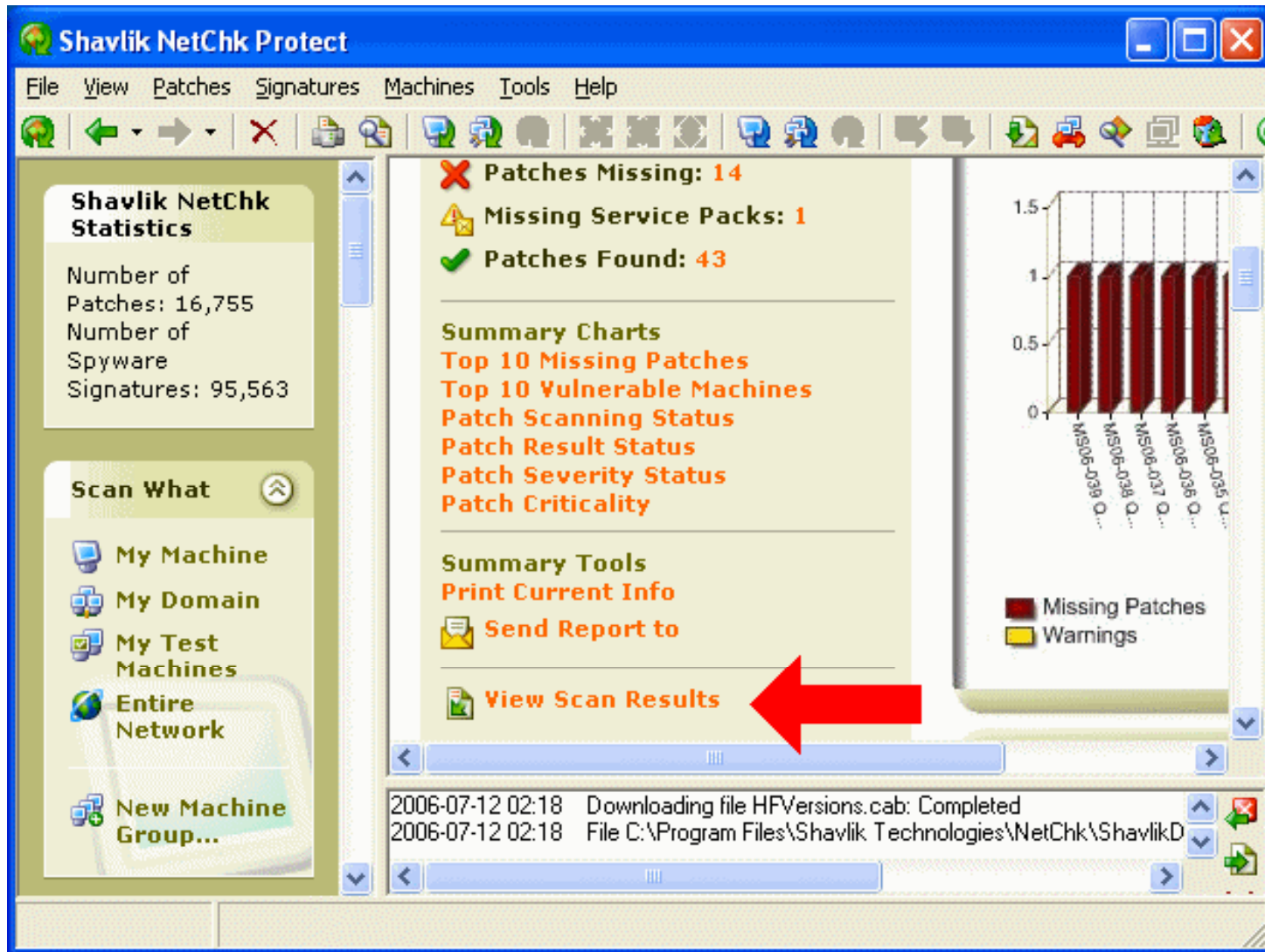
Features:

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

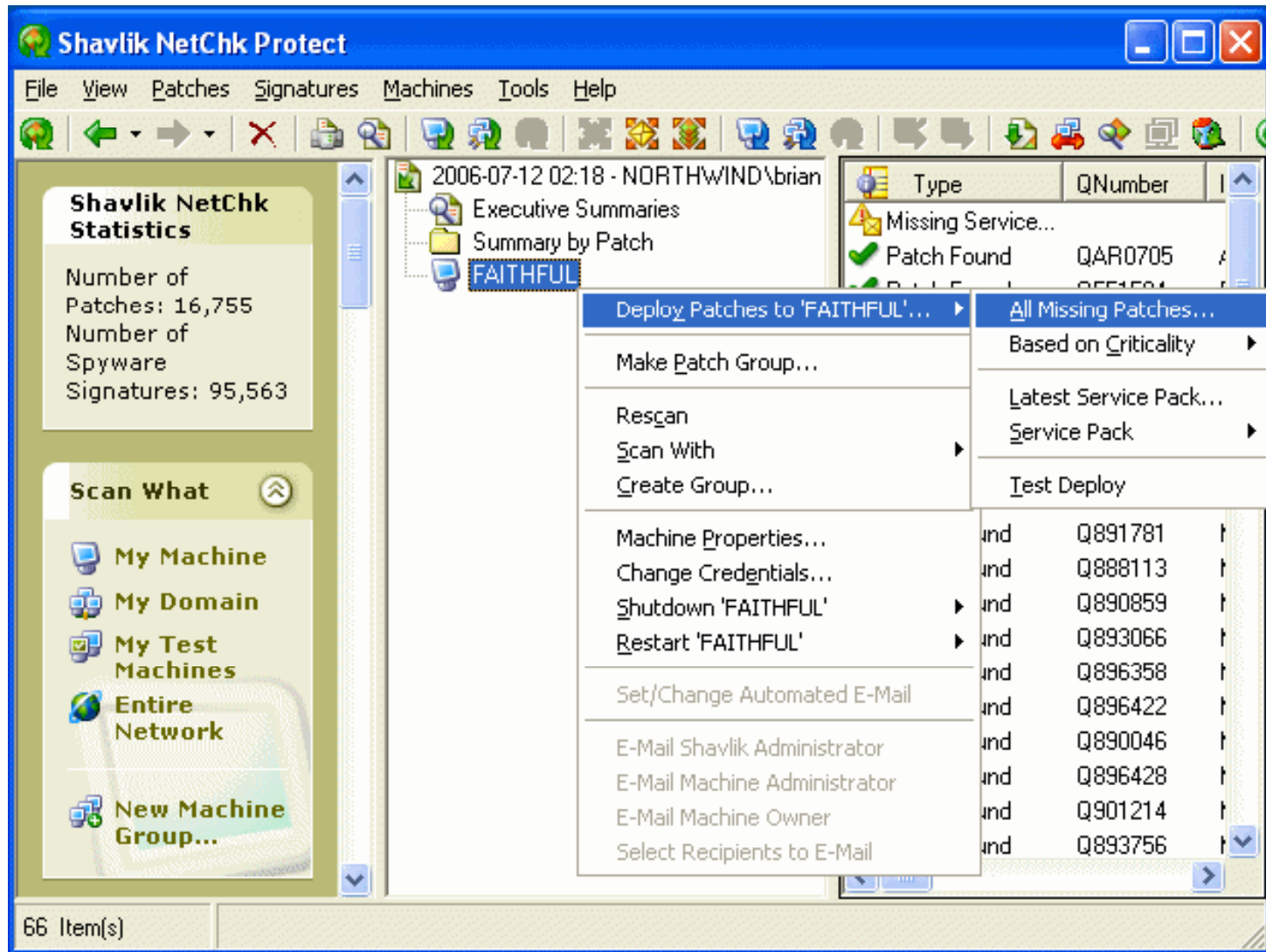
Shavlik NetChk Protect: Screenshot 1



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

Home Audit Scripts Monitor Ticketing **Patch Mgmt** Remote Cntl Backup Reports Agent System Log Off: Nick

Notes Status Machine ID Rows Select Machine Group Select View Reset

Help << < Select Page > >> 100 smc.smc < No View > Edit...

Function List

- Setup
 - Scan Machine
 - Patch Status
 - Initial Update
 - Patch History
- Schedule Update
 - Machine Update
 - Patch Update
 - Rollback
 - Automatic Update**
 - Cancel Updates
- Configure
 - Patch Approval
 - Reboot Action
 - File Source
 - Patch Alert
 - Windows Auto Update

Automatically apply all new patches and updates at the scheduled time of day.

Set Auto Every day at 3 am :00 Stagger by 5 min. Cancel

Skip if machine offline

Select All Skip if machine offline
 Unselect All Machine.Group ID Auto update time

<input checked="" type="checkbox"/>	<input type="checkbox"/>	KServer	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	kcheck01.smc.smc	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	kcheck02.smc.smc	

Powered by Kaseya - Copyright © 2000-2006 Kaseya. All rights reserved.

Kaseya Patch Management: Screenshot 2

Home Audit Scripts Monitor Ticketing **Patch Mgmt** Remote Cntl Backup Reports Agent System Log Off: Nick

Notes Status Machine ID Rows Select Machine Group Select View Reset

Help << < Select Page > >> 100 smc.smc < No View > Edit...

Function List

- Setup
 - Scan Machine
 - Patch Status**
 - Initial Update
 - Patch History
- Schedule Update
 - Machine Update
 - Patch Update
 - Rollback
 - Automatic Update
 - Cancel Updates
- Configure
 - Patch Approval
 - Reboot Action
 - File Source
 - Patch Alert
 - Windows Auto Update

Verify each machine's configuration successfully downloads and installs patches.

Test Cancel Auto Refresh Table **WARNING:** Test cancels any pending patch in progress. The system resets test results every time [File Source](#) or [Set Credential](#) changes.

[Select All](#) [Unselect All](#) **Installed** **Missing** **Missing** **Pending** **User Not** **Failed** **Test**

	Machine.Group ID	Patches Approved	Denied Patches	Logged In	Patches	Results
<input checked="" type="checkbox"/>	kcheck01.smc.smc	41	52	-	-	Passed
<input checked="" type="checkbox"/>	kcheck02.smc.smc	41	52	-	-	Untested

Powered by Kaseya - Copyright © 2000-2006 Kaseya. All rights reserved.

Kaseya Patch Management: Screenshot 3

Home Audit Scripts Monitor Ticketing **Patch Mgmt** Remote Cntl Backup Reports Agent System Log Off: Nick

Notes Status Machine ID Rows Select Machine Group Select View Reset

Help << < Select Page > >> 100 smc.smc < No View > Edit...

Function List

- Setup
 - Scan Machine
 - Patch Status
 - Initial Update
 - Patch History
- Schedule Update
 - Machine Update
 - Patch Update
 - Rollback
 - Automatic Update
 - Cancel Updates
- Configure
 - Patch Approval
 - Reboot Action**
 - File Source
 - Patch Alert
 - Windows Auto Update

Apply Specify how to reboot after applying new patches and updates.

- Reboot immediately after update.
- Reboot every day at 12 am :00 after install.
- Warn user that machine will reboot in 5 minutes (without asking permission).
- Skip reboot if user logged in.
- If user logged in ask to reboot every 5 minutes until the reboot occurs. Reboot if user not logged in.
- If user logged in ask permission. Reboot if no response in 5 minutes. Reboot if user not logged in.
- If user logged in ask permission. Do nothing if no response in 5 minutes. Reboot if user not logged in.
- Do not reboot after update. Email when reboot required.

[Select All](#) [Unselect All](#)

Machine.Group ID	Reboot action
<input type="checkbox"/> KServer	Do not reboot. Send email to bsn@bellcpa.com after update
<input type="checkbox"/> kcheck01.smc.smc	Ask - Reboot if user does not respond in 5 minutes
<input type="checkbox"/> kcheck02.smc.smc	Ask - Reboot if user does not respond in 5 minutes

Powered by Kaseya - Copyright © 2000-2006 Kaseya. All rights reserved.

Tool: IBM Tivoli Configuration Manager

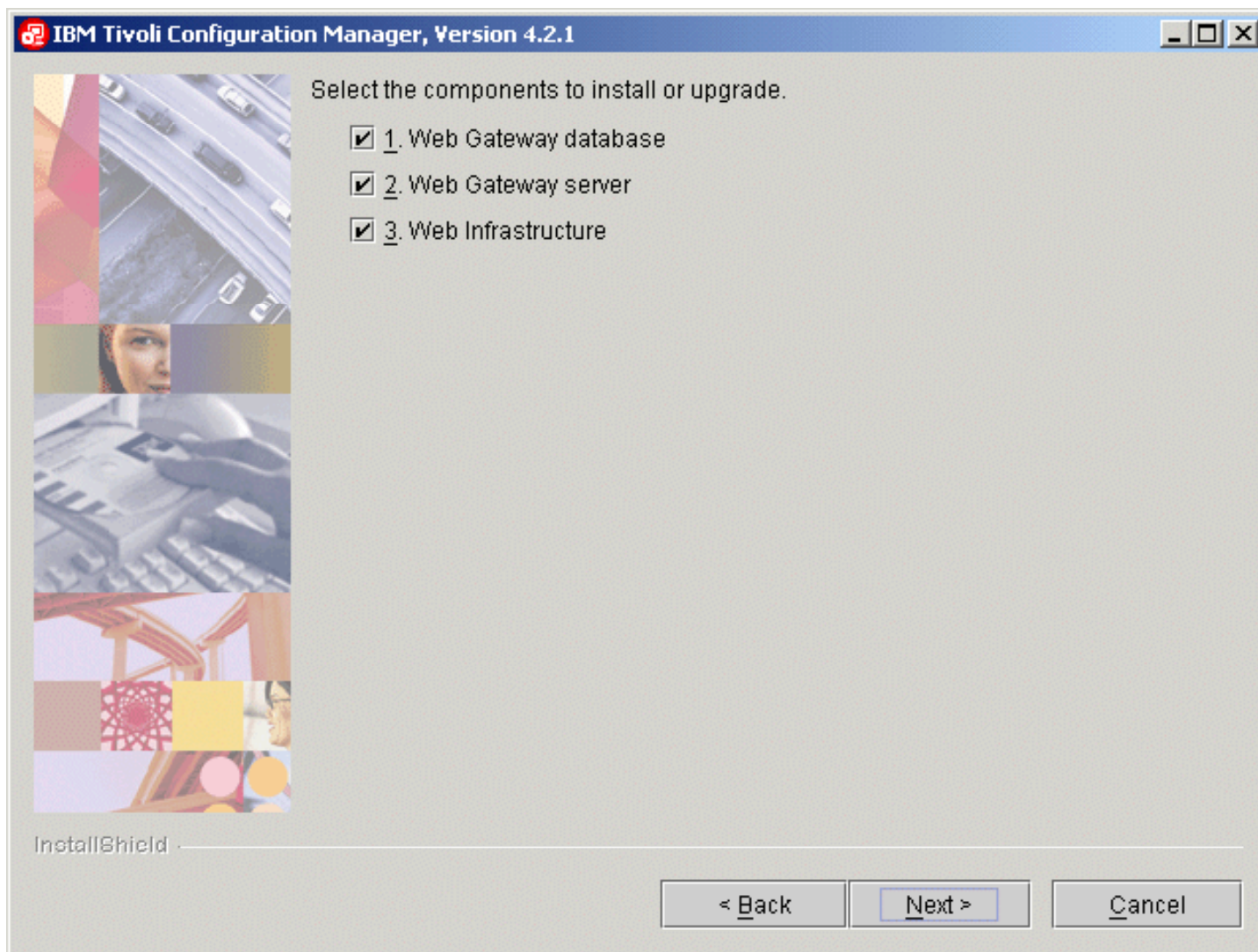
IBM's configuration manager provides Microsoft client and server software patch automation capabilities in distributed environments

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

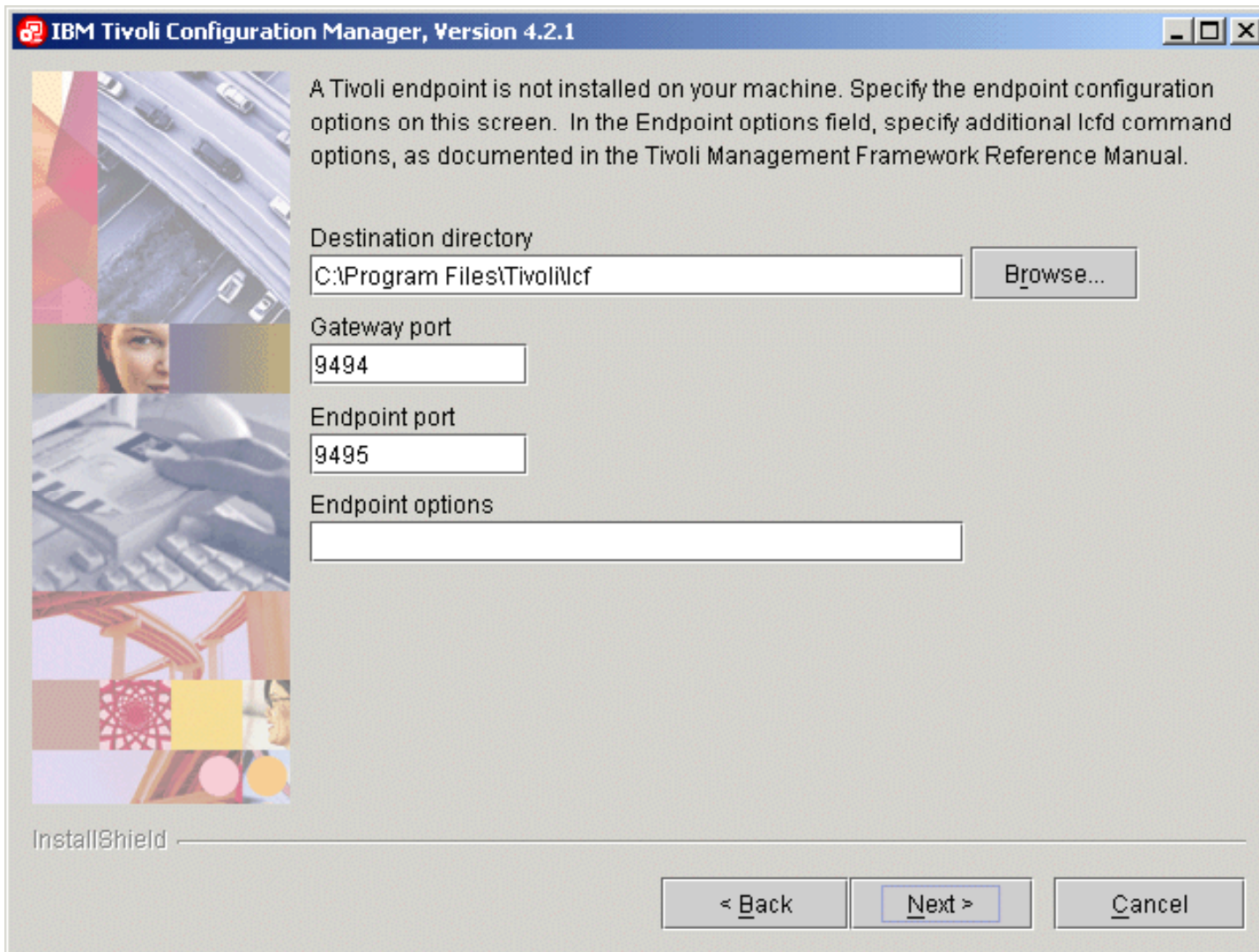
Features:

- 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

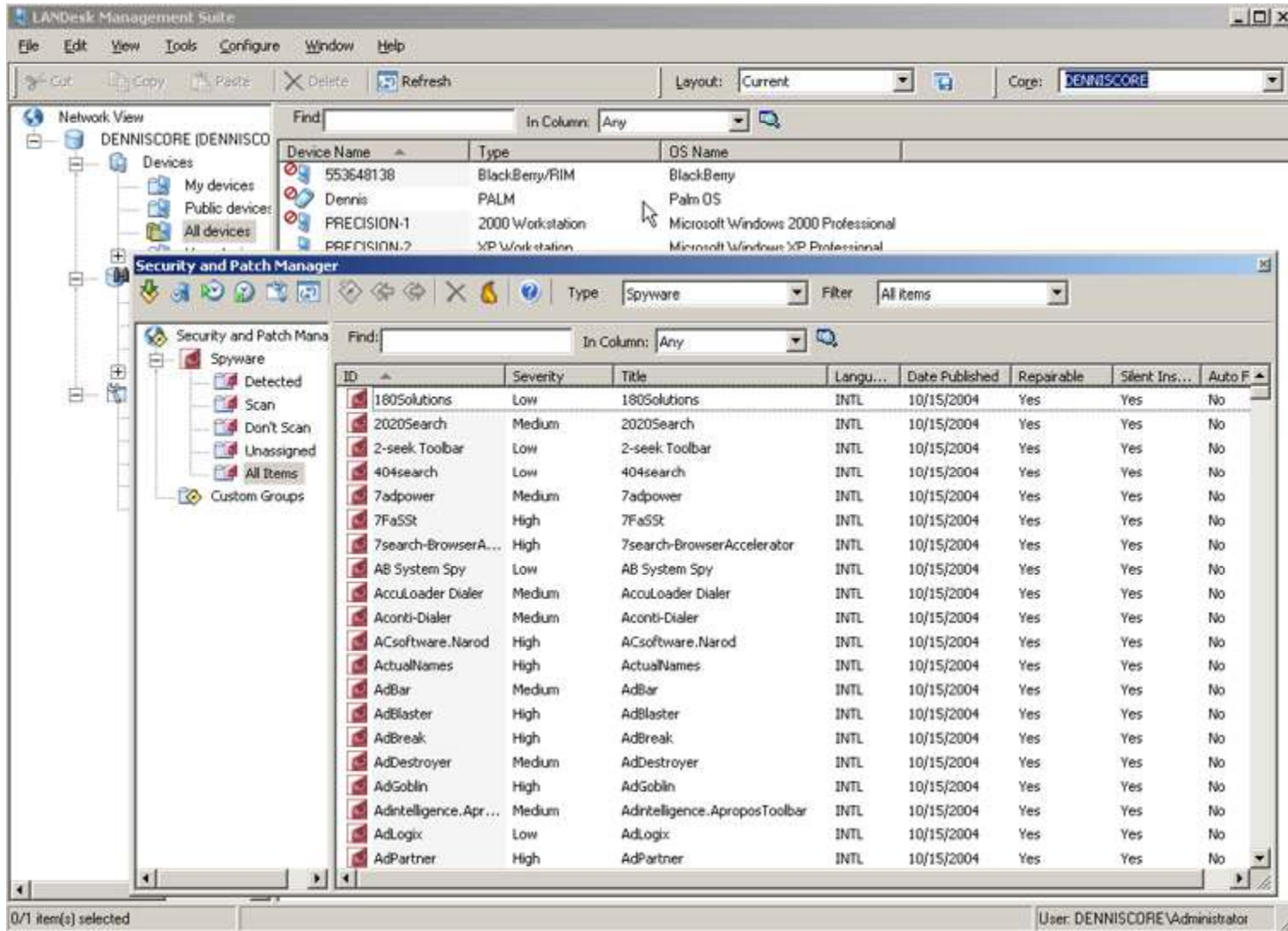
It scans managed devices to identify application and operating system vulnerabilities

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)

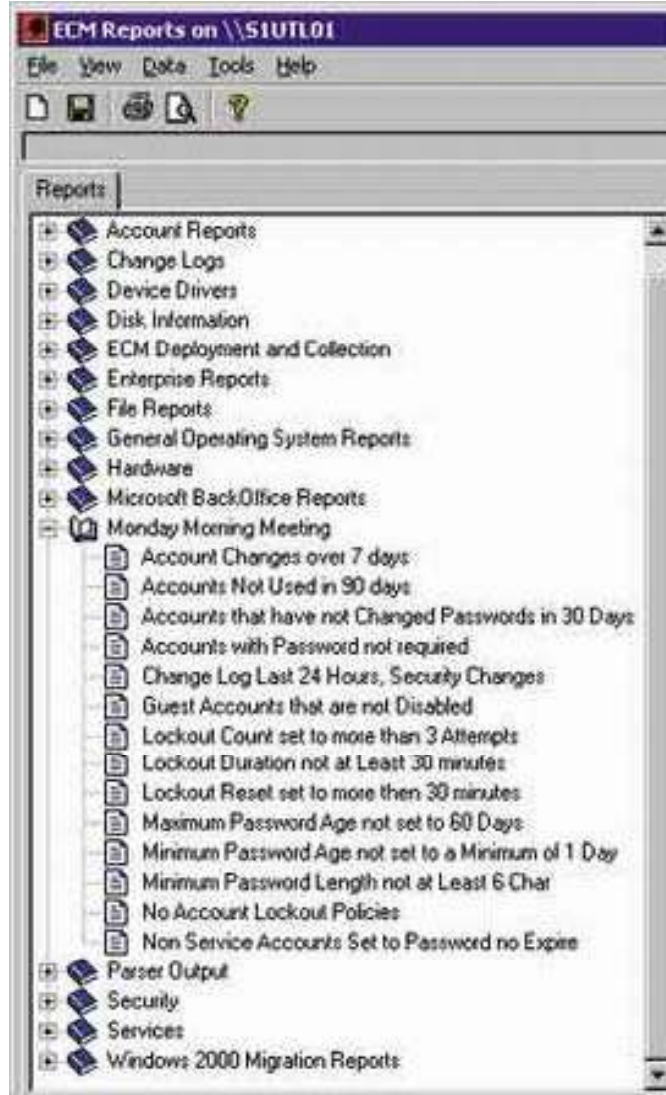
ECM centralizes and automates the monitoring, managing and auditing of hardware and software configurations across Windows, UNIX, and Linux platforms

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

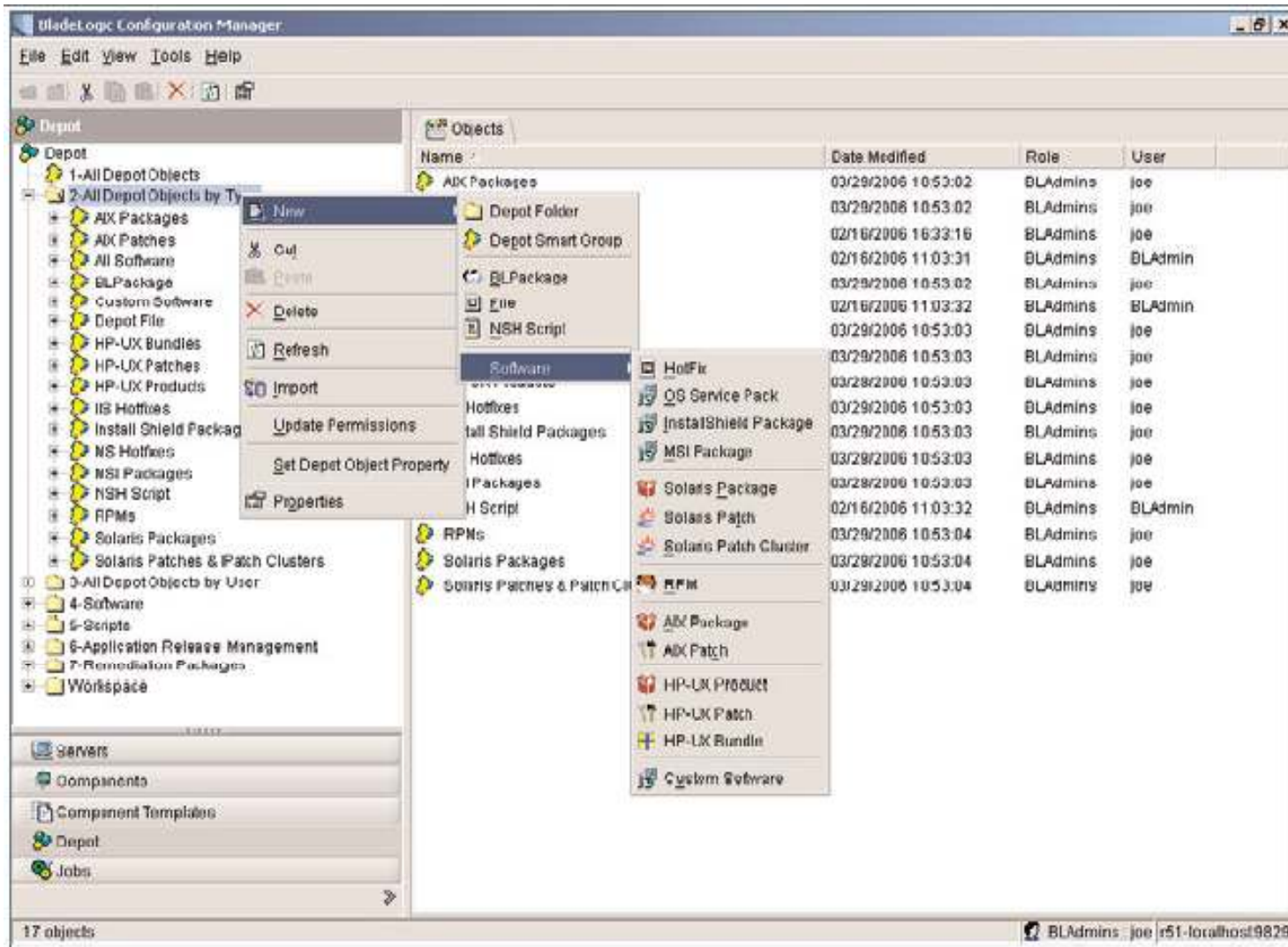
It features a cross-platform command line interface that supports a single-sign on using a range of authentication protocols

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

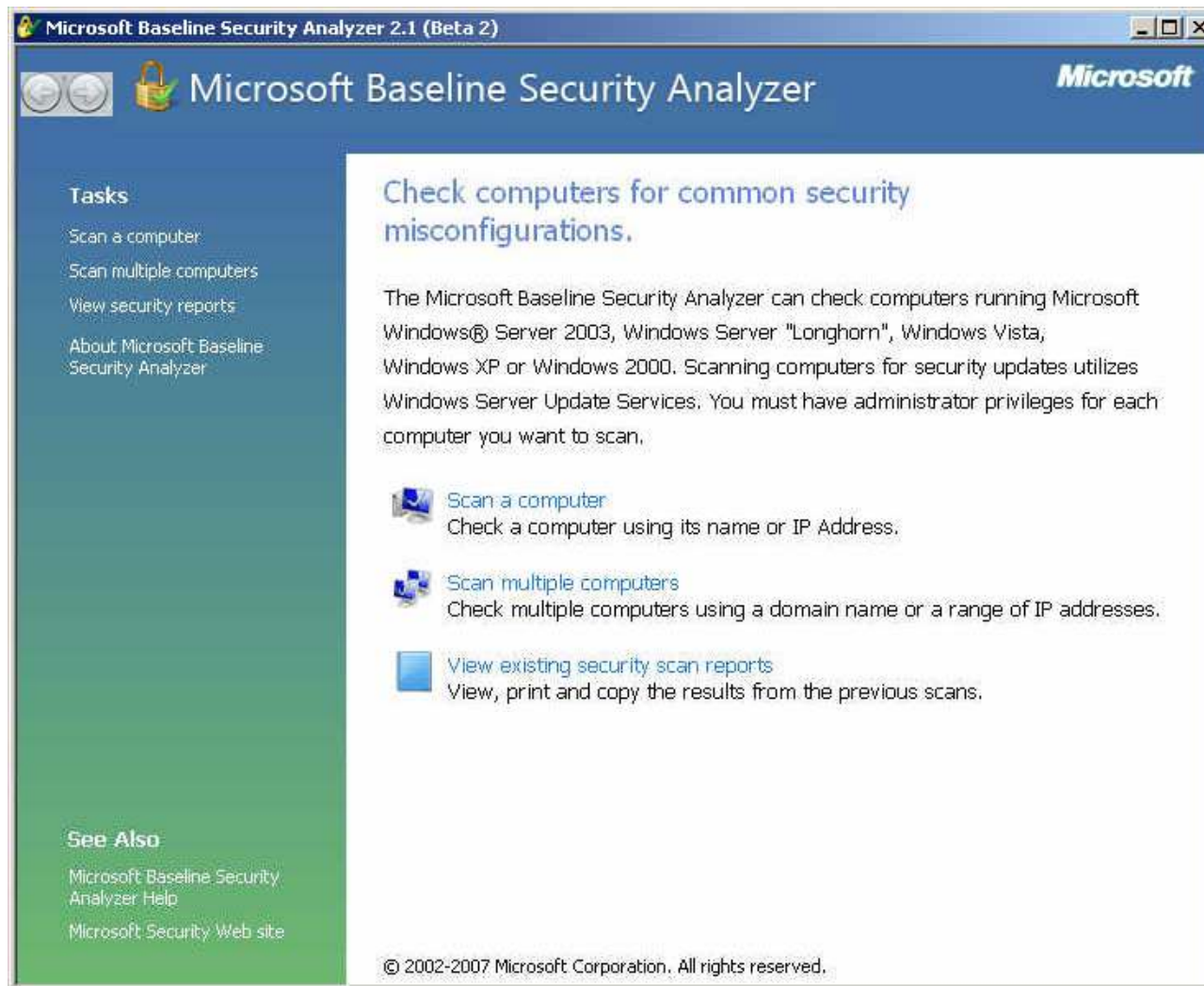
It scans and reports on updates designated as critical security updates by the Windows Update site

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] [/?]
```

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

```
C:\WINNT\System32\cmd.exe

C:\Documents and Settings>cd..

C:\>cd temp

C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is 40A6-99A6

Directory of C:\temp

11/26/2001  04:19a      <DIR>          -
11/26/2001  04:19a      <DIR>          ..
06/26/2001  03:36p           37,648 qchain.exe
10/24/2001  02:24p           10,272 readme.txt
08/14/2001  01:44p           13,346 HFNetChk License.txt
10/11/2001  04:57p          338,296 hfnetchk.exe
12/02/2001  11:53a          1,012,585 mssecure.xml
12/02/2001  12:12p      <DIR>          artiff
12/02/2001  12:01p          162,552 Q296185_W2K_SP3_x86_en.EXE
12/02/2001  11:59a          417,736 rbupdate.exe
              7 File(s)          1,992,435 bytes
              3 Dir(s)  26,061,668,352 bytes free

C:\temp>q296185_W2K_SP3_x86_en.exe -z
```


Qchain: Screenshot 2

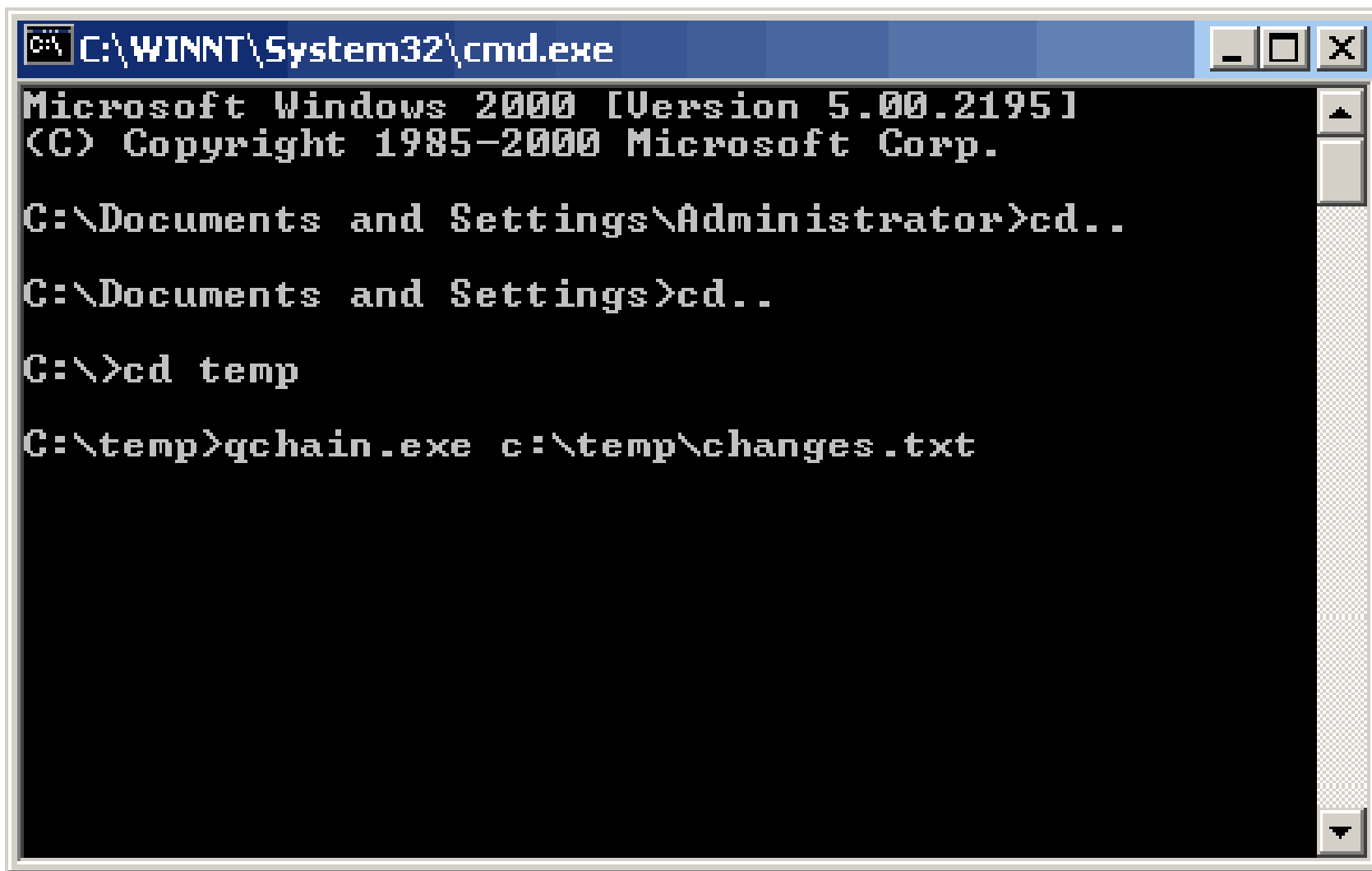
```
C:\WINNT\System32\cmd.exe
C:\Documents and Settings\Administrator>cd..
C:\Documents and Settings>cd.
C:\Documents and Settings>cd..
C:\>cd temp
C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is 40A6-99A6

Directory of C:\temp

11/26/2001  04:19a      <DIR>          .
11/26/2001  04:19a      <DIR>          ..
06/26/2001  03:36p           37,648 qchain.exe
10/24/2001  02:24p           10,272 readme.txt
08/14/2001  01:44p           13,346 HFNetChk License.txt
10/11/2001  04:57p          338,296 hfnetchk.exe
12/02/2001  11:53a       1,012,585 mssecure.xml
           5 File(s)          1,412,147 bytes
           2 Dir(s)     26,086,359,040 bytes free

C:\temp>
```

Qchain: Screenshot 3



```
C:\WINNT\System32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>cd..

C:\Documents and Settings>cd..

C:\>cd temp

C:\temp>qchain.exe c:\temp\changes.txt
```

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 trail of every action and step taken on each computer during the patch management process

BigFix Enterprise Suite (BFS): Screenshot 1

The screenshot displays the BigFix Enterprise Console interface. At the top, a window title reads "BigFix Enterprise Console - [Fidlet 'MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - MDAC 2.80 - Windows 2000/XP']". The main area is divided into a left-hand navigation pane and a central content area.

Navigation Pane: Shows "All Relevant Fidlet Messages (49)" with a tree view categorized by severity: <Unspecified> (32), Low (3), Moderate (1), Important (6), and Critical (7). Other options include "By Site" and "By Category".

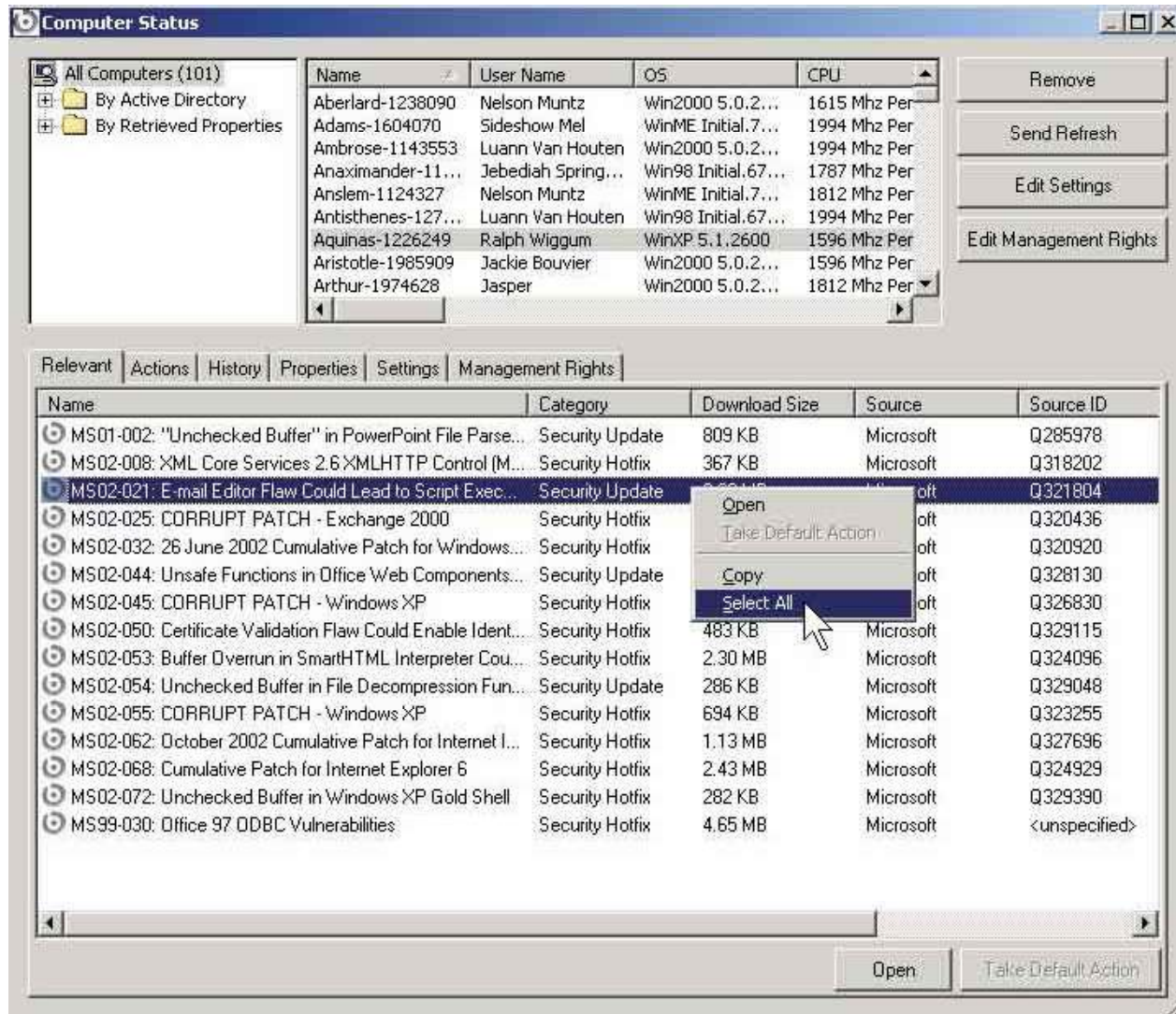
Message List: A table of messages with columns for Name, Source Sev..., and Site. The list includes several entries for MS06-014 and MS06-015, all marked as Critical.

Message Details: The selected message is "Fidlet: MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - MDAC 2.80 - Windows 2000/XP" with a severity of Critical. It shows "0 Relevant Computers" and "0 Open Actions".

Description: The description area features a "BIGFIX Patch Management Patches for Windows" banner. Below it, the title "MS06-014: Vulnerability in the MDAC Function Could Allow Code Execution - MDAC 2.80 - Windows 2000/XP" is displayed. The text explains that Microsoft has released a patch for a vulnerability in the Microsoft Data Access Components (MDAC) Function, which could allow an attacker with administrative rights to take complete control of the system. It also notes that affected computers will report as 'Pending Restart' and that a future Update Rollup may include the update.

Status Bar: At the bottom, it shows "Ready" on the left and "Connected to database 'bfenterprise' as user 'EvaluationUser'" on the right.

BigFix Enterprise Suite (BFS): Screenshot 2



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

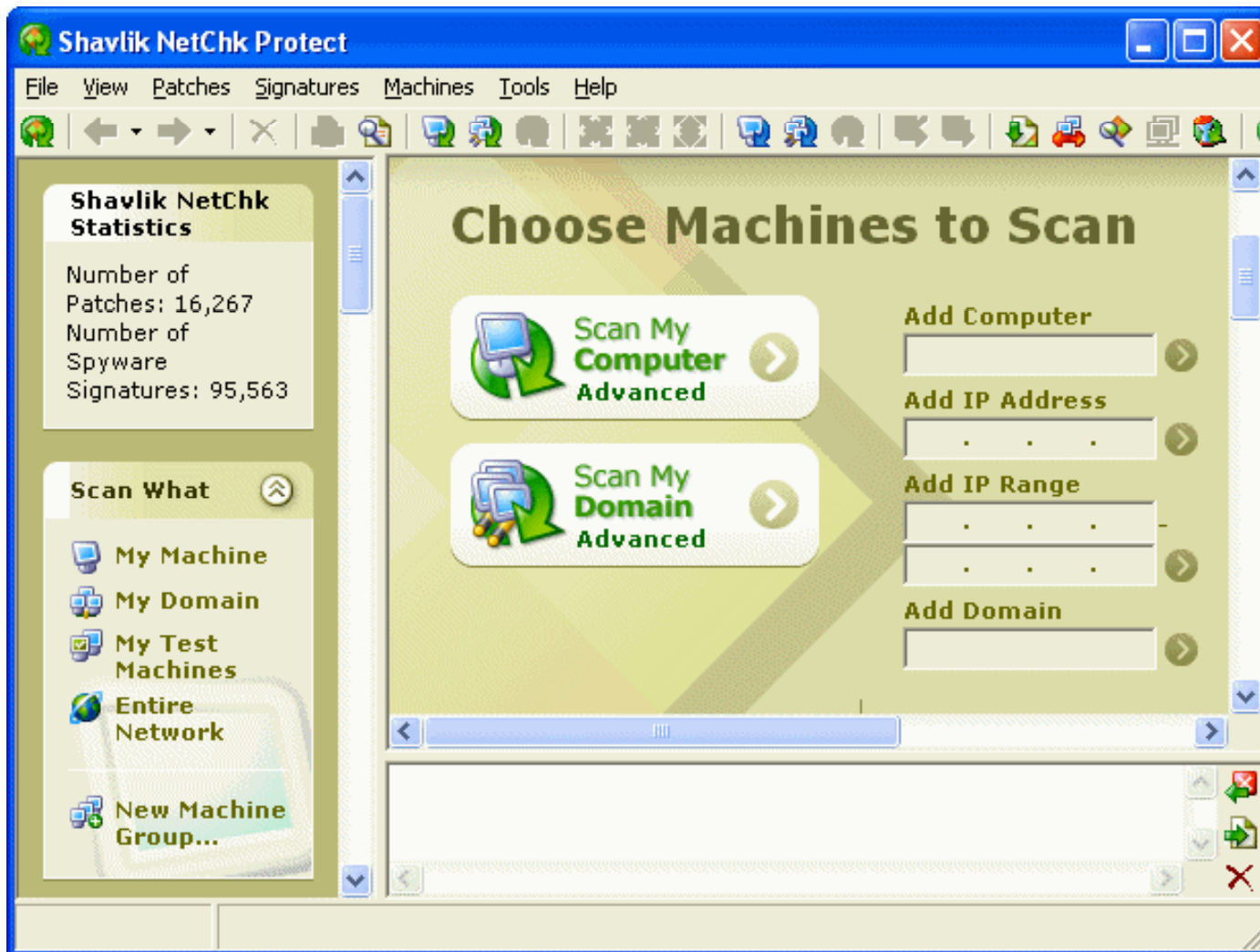
Features:

- 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

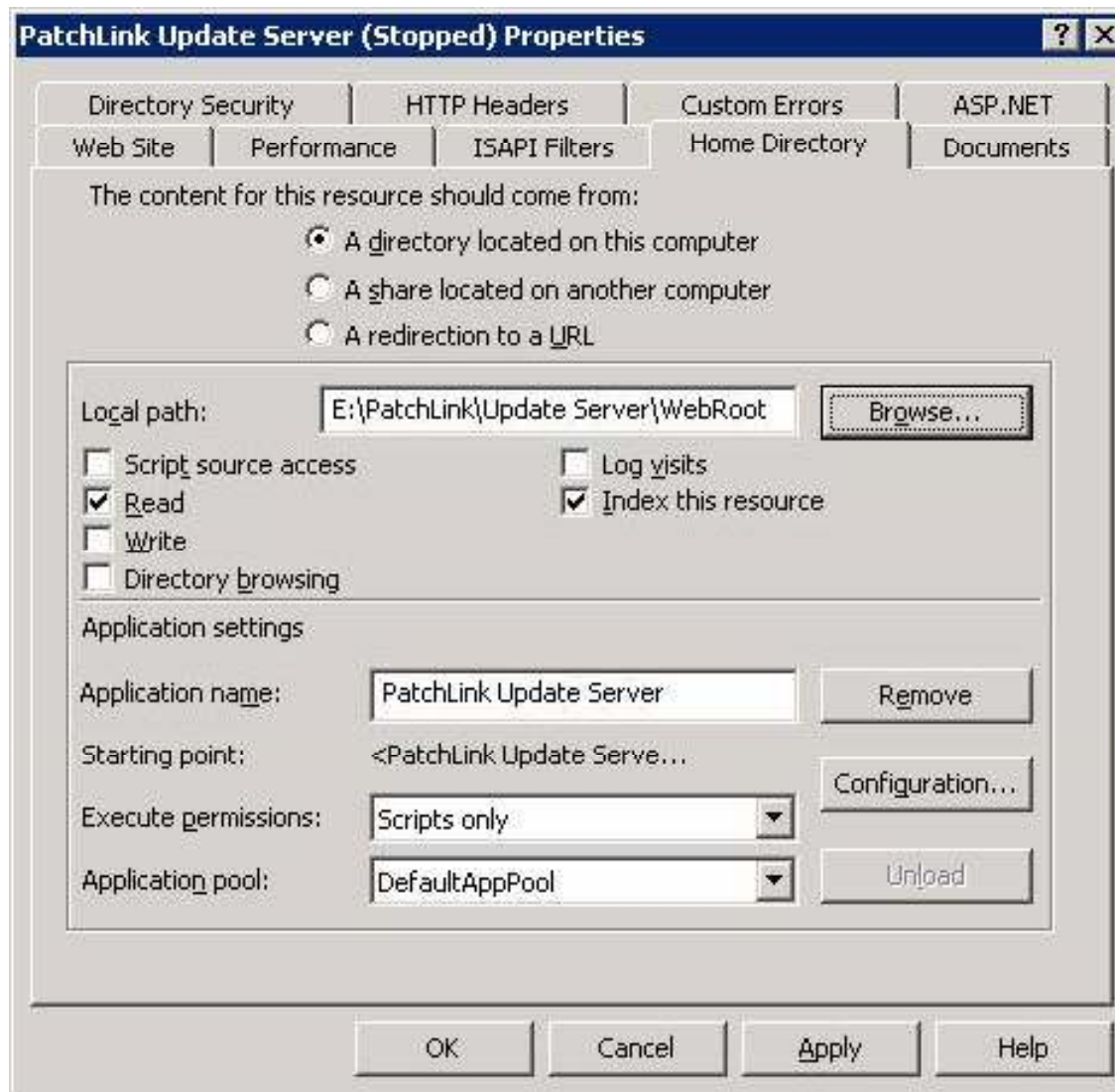
It scans networks for security holes using fingerprint technology

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

The screenshot displays the PatchQuest interface for a scan result. The main content area features a 'Product Summary' table and a list of updates.

Product Name	Service Packs	Available Patches	Missing Patches	Informational Items	Obsolete Patches
All	11	66	12	4	25
Windows 2000 Professional SP4 (x86)	1	25	10	2	11
Excel 2000 Gold	2	1	0	0	0
Internet Explorer 6 Gold	2	1	0	0	0
MSMC 2.6 SP2	1	1	0	0	0
MSXML 2.6 SP2	2	0	0	0	0
msxml 3.0 SP1	1	0	0	0	0
MSXML 4.0 SP2	1	0	1	0	1
MSXML 4.0 Gold	1	0	1	0	1
Office 2000 Gold	2	2	0	0	0
Outlook 2000 Gold	2	0	0	0	0
Outlook Express 6.0 Gold	2	0	0	0	1
PowerPoint 2000 Gold	2	0	0	0	0
SQL Server 2000 Gold	2	2	0	1	0
Windows Media Player 6.4 for Windows 2000 SP4	1	1	0	0	0
Word 2000 Gold	2	0	0	1	1
Word 7.0 Gold	1	0	0	0	0

Agent	Agent Status	Update Status
PatchQuest Agent	Running	Up-to-date

Patch Status	Bulletin ID	Patch Name	Installation Status	Download Status	Severity
✓	MSRT-001	Windows-KB900326-EM-Exec...	NA	✓	Low
✓	MSRT-044	rtToWeb.exe	NA	✓	Low
✓	MSRT-070	JavaPlus.exe	NA	✓	Low
✓	MS06-078	WindowsMedia6-KB929776-x86-EM-Exec...	NA	✓	High
✗	MS06-077	Windows2000-KB920173-x86-EM-Exec...	NA	✗	High
✗	MS06-071	msxml4-KB927779-enu.exe	NA	✗	High
✗	MS06-071	msxml6-KB927777-enu-x86.exe	NA	✗	High
✗	MS06-070	Windows2000-KB924270-x86-EM-Exec...	NA	✗	High
✗	MS06-068	Windows2000-KB920172-x86-EM-Exec...	NA	✗	High

SecureCentral PatchQuest: Screenshot 2

secure | central™
PatchQuest

Feedback | About | Personalize | Help | License | Logout (admin)

Home | **Systems** | System Groups | Patch Information | Patch Groups | Reports | Settings | Support

Quick Search | Update DB | Add System | Scan System | Deploy Patches | Deploy Service Packs | Recent Tasks

Systems

- All Systems
- Windows
- Red Hat
- Debian

Agent Update Status

- Windows
- Linux

Bookmarks

No Bookmark Available. [Add new?](#)

Quick Note

View missing and available patches for this system. The Product Summary presents a consolidated patch view of the products assessed in the system. You can select and "Deploy" the missing patches and "Undeploy" the available ones. Use the "Download" button to select and download required patches in to the server.

Scan Result > SD-TEST3

Scan Now | Export | Print | Help

Deploy | Download | Undeploy | Add To Patch Group

Search: None like

Showing: 1 to 25 of 60

Patch Status	Bulletin ID	Patch Name	Title	Installation Status	Download Status	Severity	Superseded By	Views
<input type="checkbox"/>	MS05-037	New IES_01-KB903235-x86-ENU.exe	Vulnerability in JView Profiler Could Allow Remote Code Execution (903235)	NA		C	NA	
<input type="checkbox"/>	MS05-036	New Windows2000-KB901214-x86-ENU.EXE	Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)	NA		C	NA	
<input type="checkbox"/>	MS05-032	Windows2000-KB890046-x86-ENU.EXE	Vulnerability in Microsoft Agent Could Allow Spoofing (890046)	NA		H	NA	
<input type="checkbox"/>	MS05-031	StepByStepInteractiveTraining-KB898458-x86-ENU.exe	Vulnerability in Step-by-Step Interactive Training Could Allow Remote Code Execution (898458)	NA		H	NA	
<input type="checkbox"/>	MS05-027	Windows2000-KB896422-x86-ENU.EXE	Vulnerability in Server Message Block Could Allow Remote Code Execution (026422)	NA		C	NA	
<input type="checkbox"/>	MS05-011	Windows2000-KB885250-x86-ENU.EXE	Vulnerability in Server Message Block Could Allow Remote Code Execution (885250)	NA		C	NA	
<input type="checkbox"/>	MS05-008	Windows2000-KB890047-x86-ENU.EXE	Vulnerability in Windows Shell Could Allow Remote Code Execution (890047)	NA		H	NA	
<input type="checkbox"/>	MS05-003	Windows2000-KB871250-x86-ENU.EXE	Vulnerability in the Indexing Service Could Allow Remote Code Execution (871250)	NA		H	NA	
<input type="checkbox"/>	MS05-002	Windows2000-KB891711-x86-ENU.EXE	Vulnerability in Cursor and Icon Format Handling Could Allow Remote Code Execution (891711)	NA		C	MS05-018	
<input type="checkbox"/>	MS05-001	Windows2000-KB890175-x86-ENU.EXE	Vulnerability in HTML Help Could Allow Code Execution (890175)	NA		C	MS05-026	
<input type="checkbox"/>	MS04-044	Windows2000-KB885835-x86-ENU.EXE	Vulnerabilities in Windows Kernel and LSASS Could Allow Elevation of Privilege (885835)	NA		H	NA	
<input type="checkbox"/>	MS04-043	Windows2000-KB873339-x86-ENU.EXE	Vulnerability in HyperTerminal Could Allow Code Execution (873339)	NA		H	NA	
<input type="checkbox"/>	MS04-041	Windows2000-KB885836-x86-ENU.EXE	Vulnerability in WordPad Could Allow Code Execution (885836)	NA		H	NA	

Tool: Patch Authority Ultimate

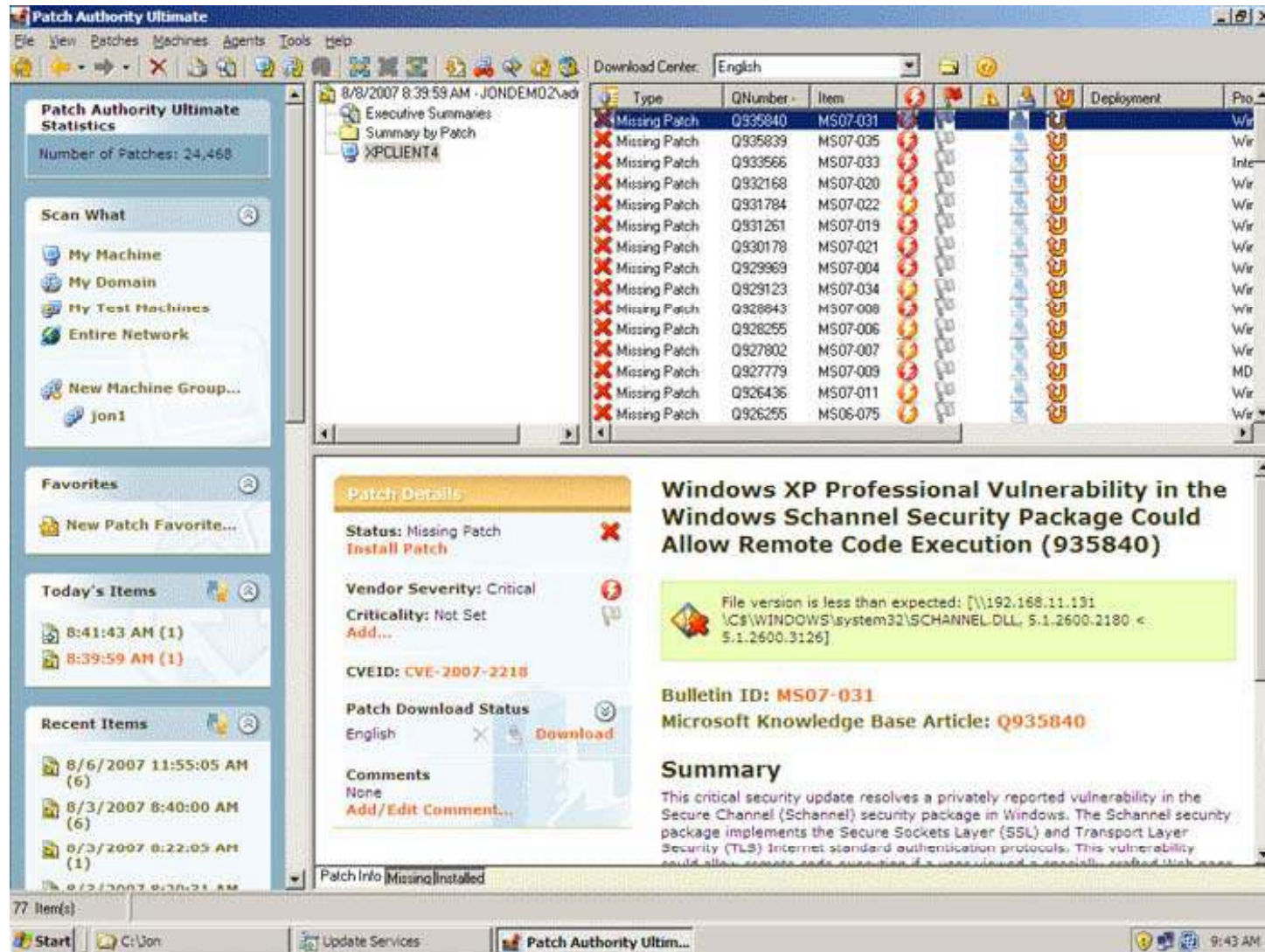
Patch authority ultimate is ScriptLogic's comprehensive and enterprise-class patch management solution

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

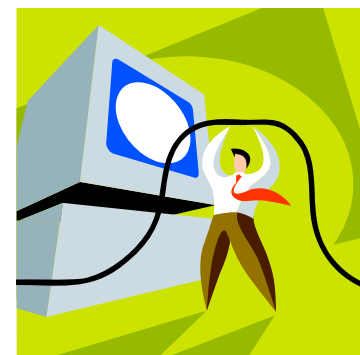


Tool: ZENworks Patch Management

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

N
Novell. ZENworks.
PATCHLINK

Home | Reports | Inventory | Packages | Computers | Groups | Users | Options | Help |
Server Time: 4/2/2004 11:14:23 AM (GMT-07:00)

Get support and the latest information about patches....

What is PatchLink Update
 Select this link to see an overview of PatchLink Update including its features and benefits...

New Users Start Here
 If you are new to PatchLink Update, select this link to see how to get up and running fast...

Help Info
 Select this link for full comprehensive help documentation about PatchLink Update...

Known Issues & Resolutions
 Select this link to see a list of known issues and release notes about this version of the PatchLink Update Server.

March 10, 2004

Microsoft Security Bulletin MS04-009

SEVERITY: Important


DATE RELEASED: March 9, 2004

SYSTEMS AFFECTED
 Office XP SP2, Office 2002 SP2

RECOMMENDATION
 Customers should install the patch at

Comprehensive Graphical Assessments:

Patch Status for all Reports



Select to Change Graph:

- Patch Status for all Computers
- Patch Status for all Reports
- Status for all Computers
- Baseline Status for all Groups

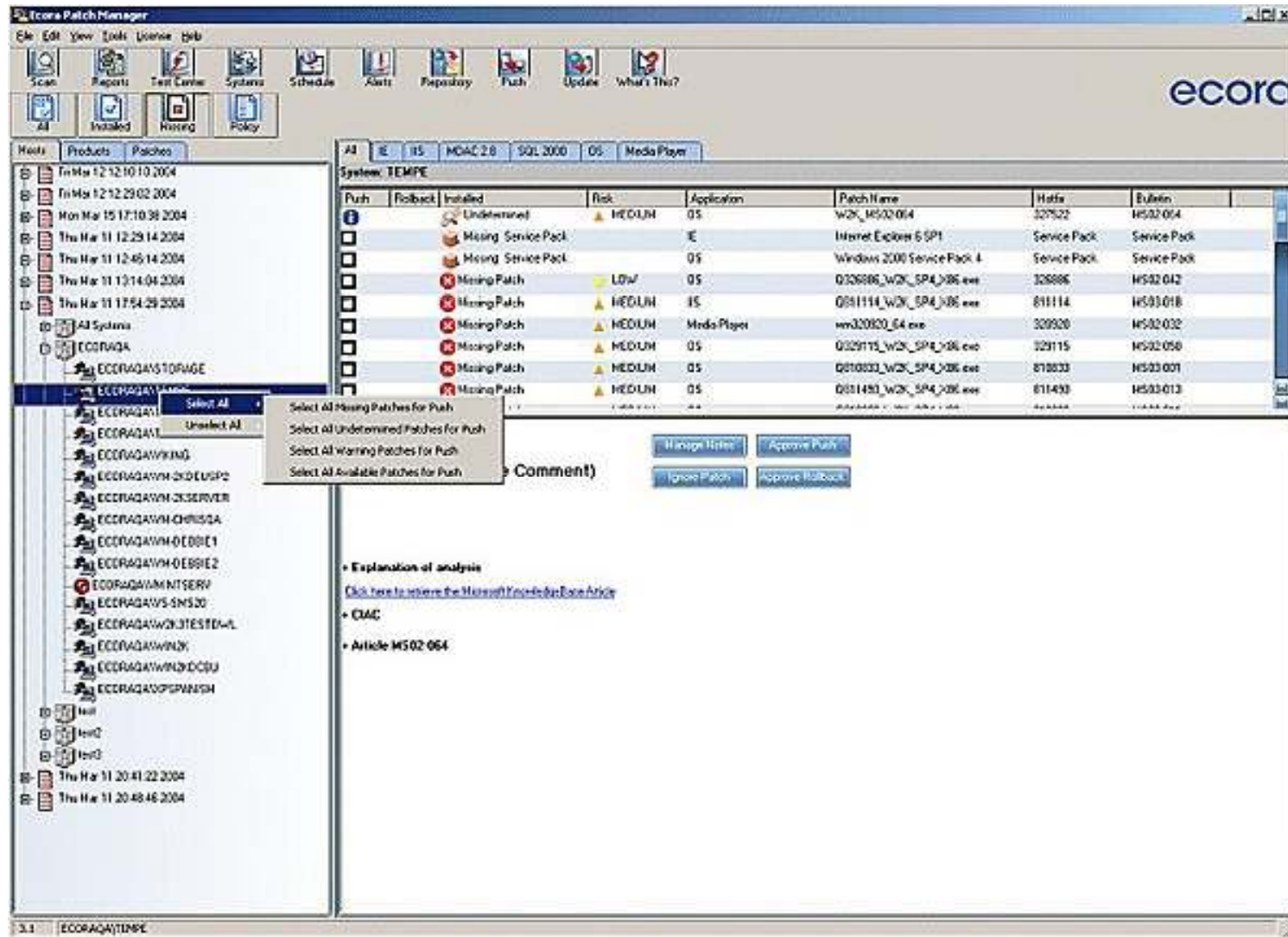
patchlink

Ecora 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

Missing Patches - Microsoft Internet Explorer

File Edit View Favorites Tools Help

ecora Missing Patches [Print Report...](#)

Page 1 of 2 1-30 of 46 items shown

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

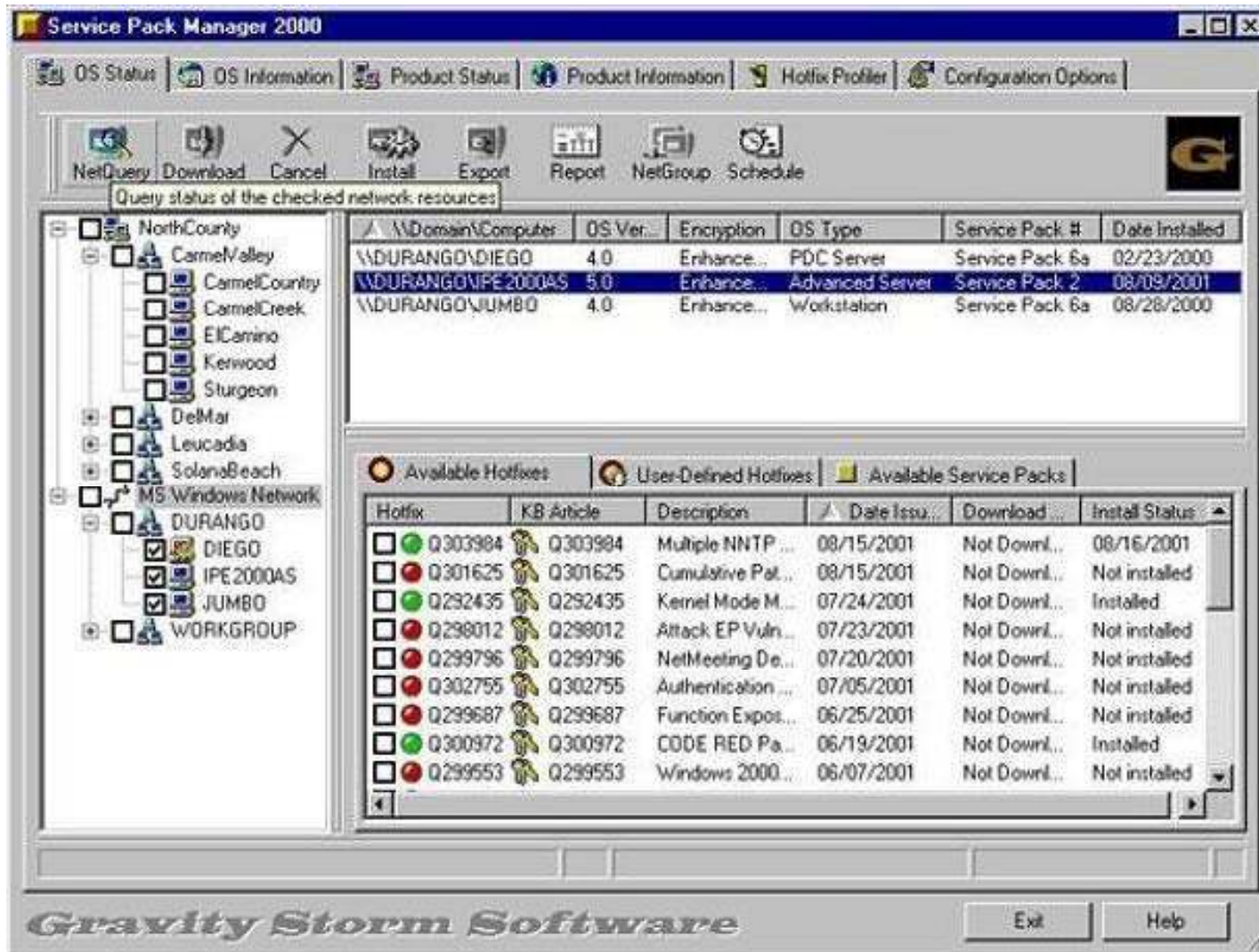
It allows to remotely detect, track, monitor, and install Windows NT/2000/XP/2003 Service Packs and Hotfixes on the enterprise networks from a central console

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

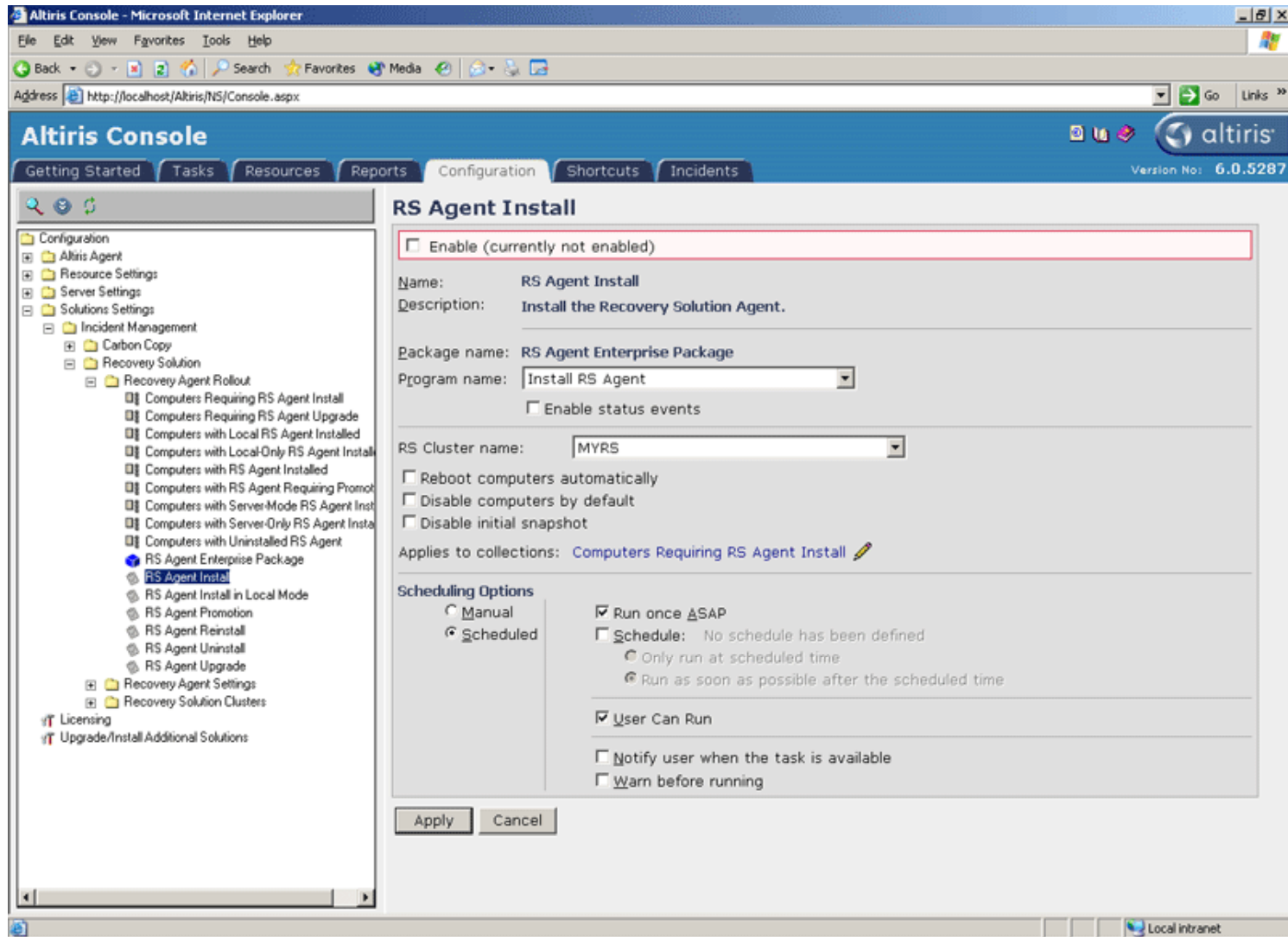
Altiris Patch Management Solution software proactively manages patches and software updates by automating the collection, analysis, and delivery of patches across your enterprise

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

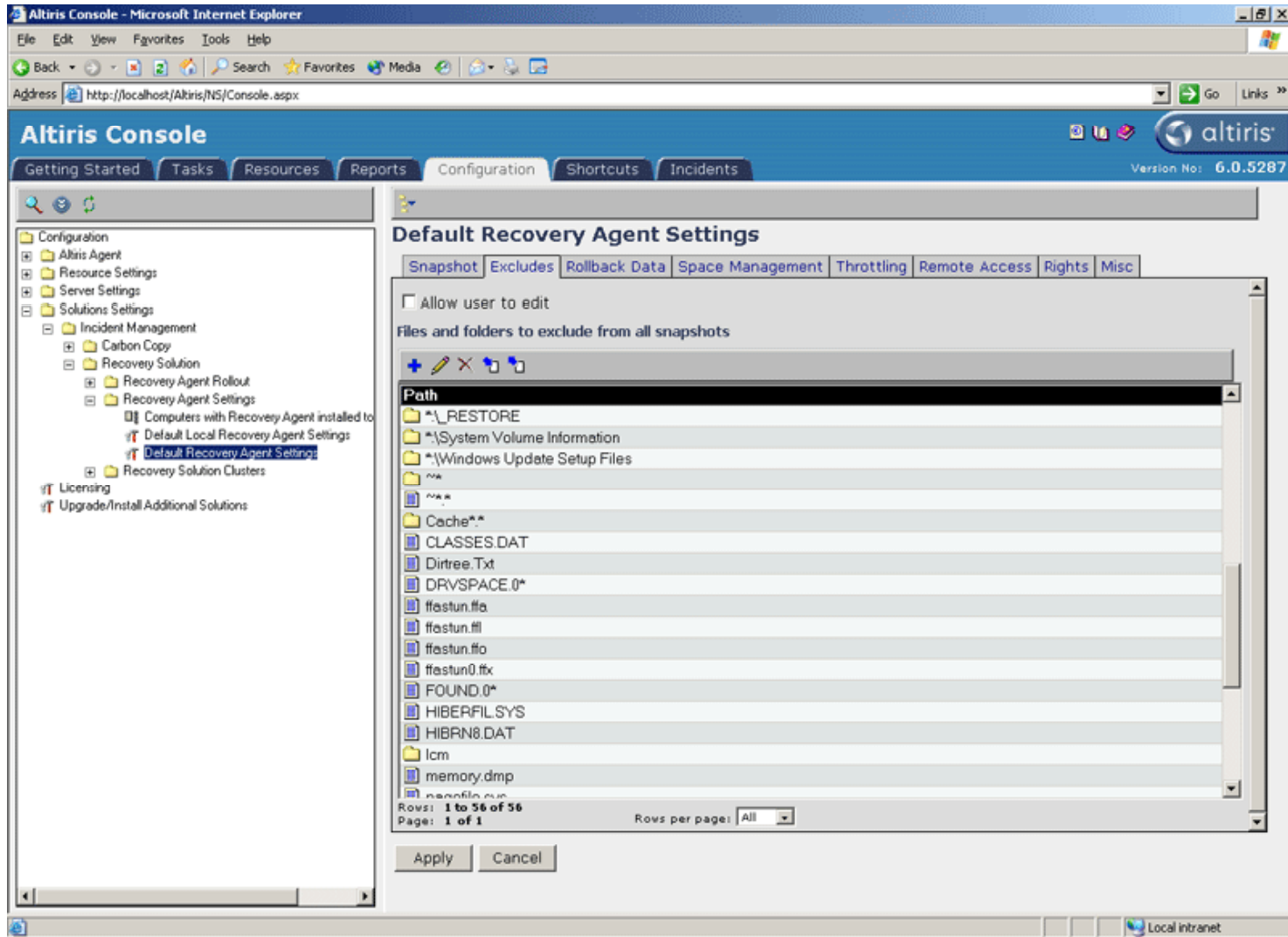
It provides improved functionality in the analysis, collection, and distribution of OS and application updates

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

BMC Configuration Management Report Center

Applications ▾ Common Tasks ▾ Home About Logout

Queries Query Library **Policy Compliance** Status Hide intro text Help

Compliance Target View

From this page you can see the subscription targets in your directory and the policy compliance associated for a target. <time zone information needed, console time vs. end-point time.>

Targets previous 1-20 of 60 next

Search for: Go

Do not search sub-containers

Home > Marimba > US

- Development
- Engineering**
- Finance
- Field Services
- HR
- IT
- Legal
- Marketing
- Office of CTO
- Purchasing
- Sales
- Support
- Training

Engineering View Policy

View compliance for: All policies affecting this target Show numbers Show percentages

Overall compliance: 70% 25% 5%

Policy last modified: 7/15/03 8:00AM
 Members checked in: 400/500

Package	Policy State	Compliance	Directly Assigned To
Emacs	Install	 80% 15% 5%	Engineering
Internet Explorer 6.0	Install	 70% 400 22%	Mountain View
Trillian	Stage	 100% 0% 0%	Mountain View
Visio	Advertise	 100% 0% 0%	Engineering
WinZip	Install	 90% 5% 5%	Mountain View

Green=Compliant Red=Non-compliant Blue=Not checked in

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



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

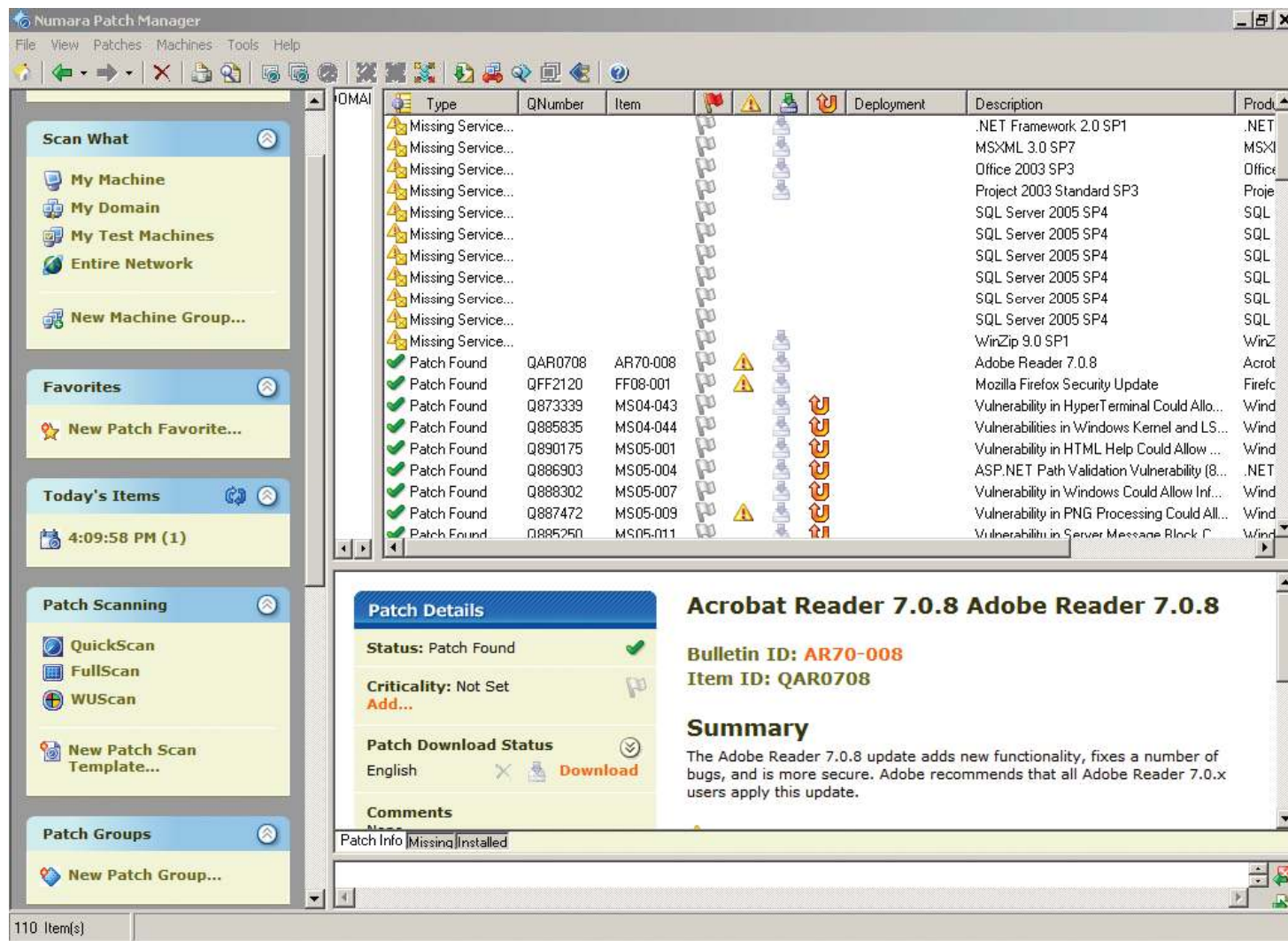
It allows you to assess the patch status of all Microsoft-based workstations as well as validate any existing patches that have been installed

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

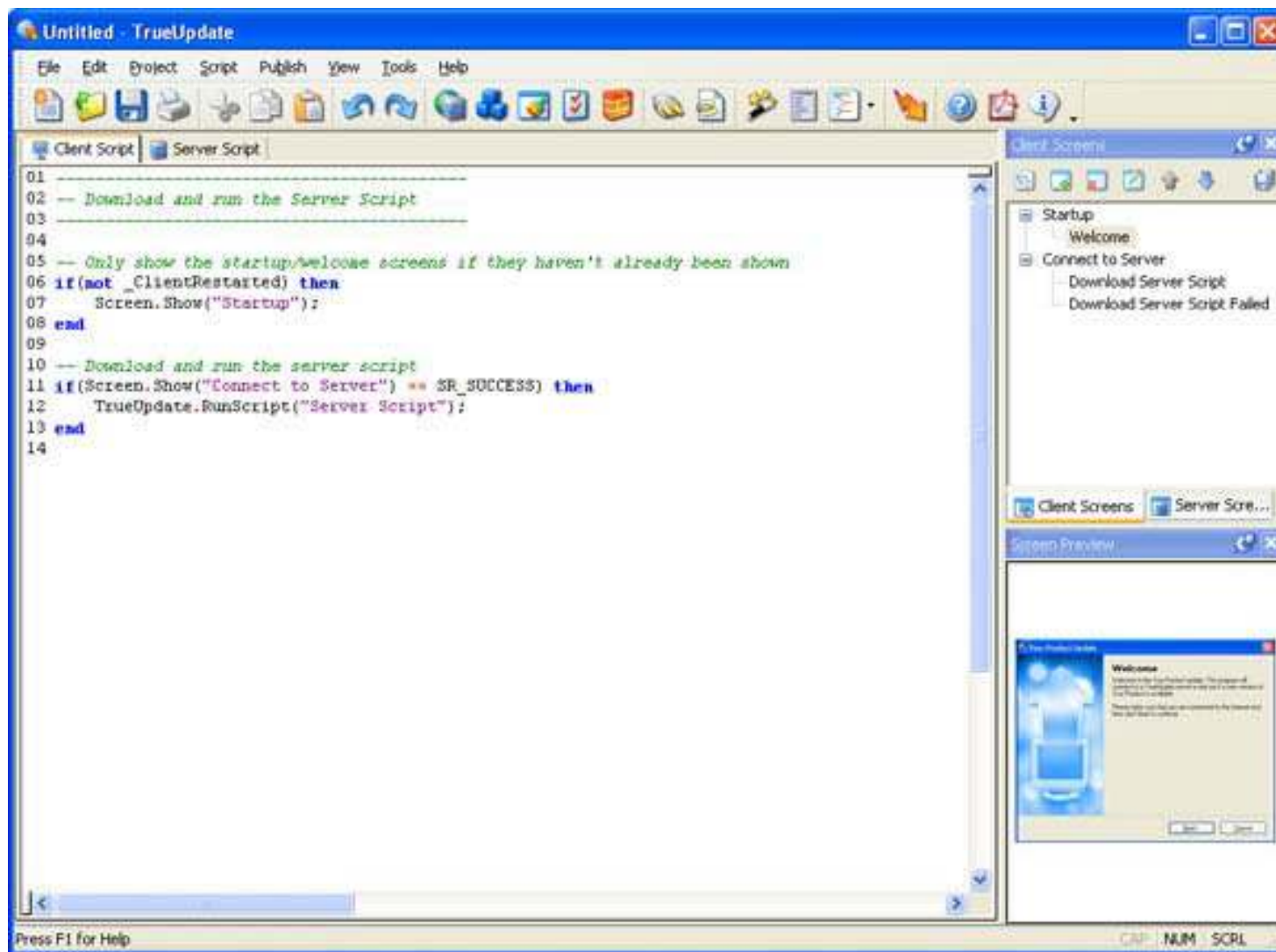
TrueUpdate is a comprehensive solution for software developers wanting to integrate automatic updating capabilities into their software applications

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

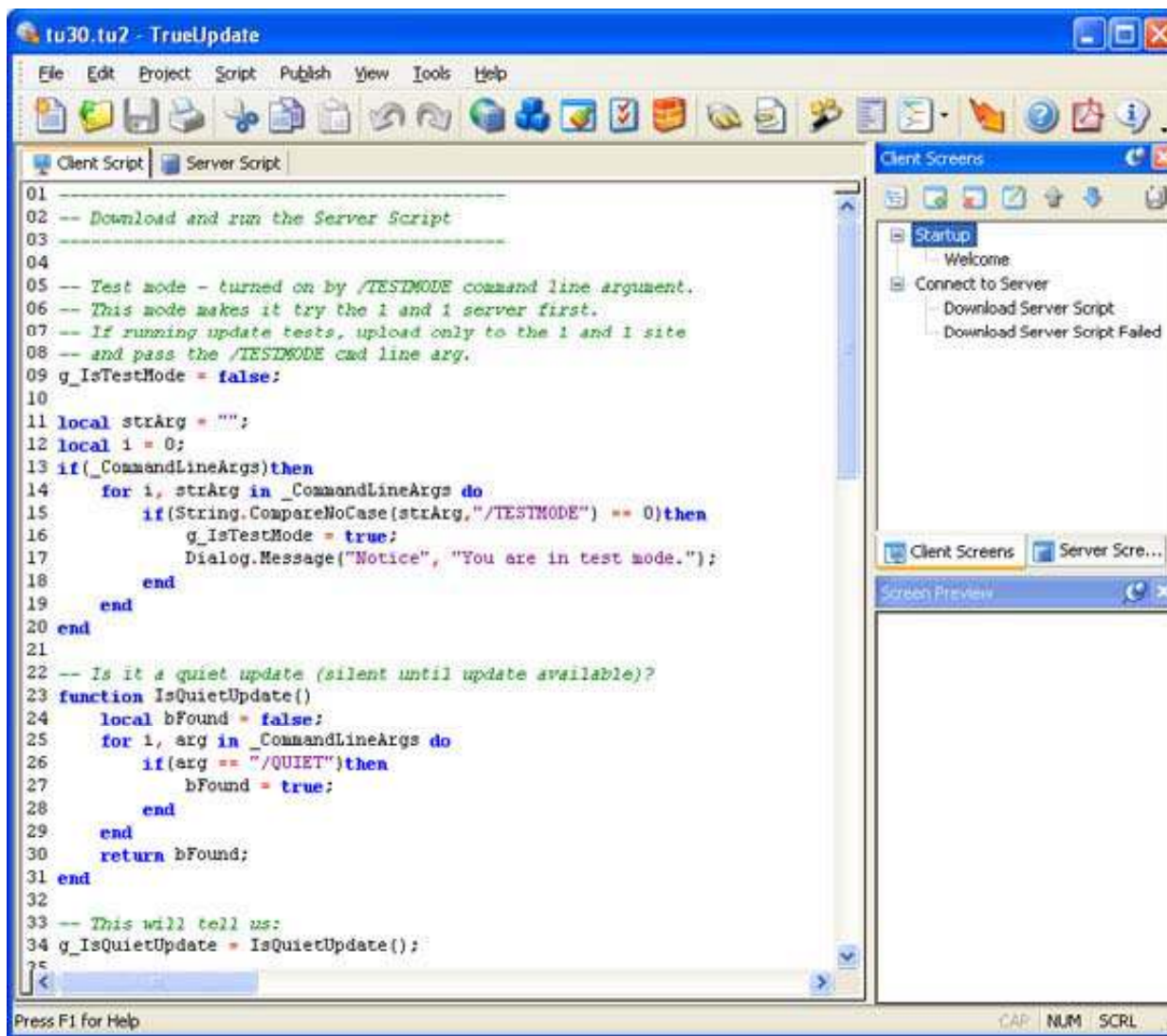
Features:

- 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



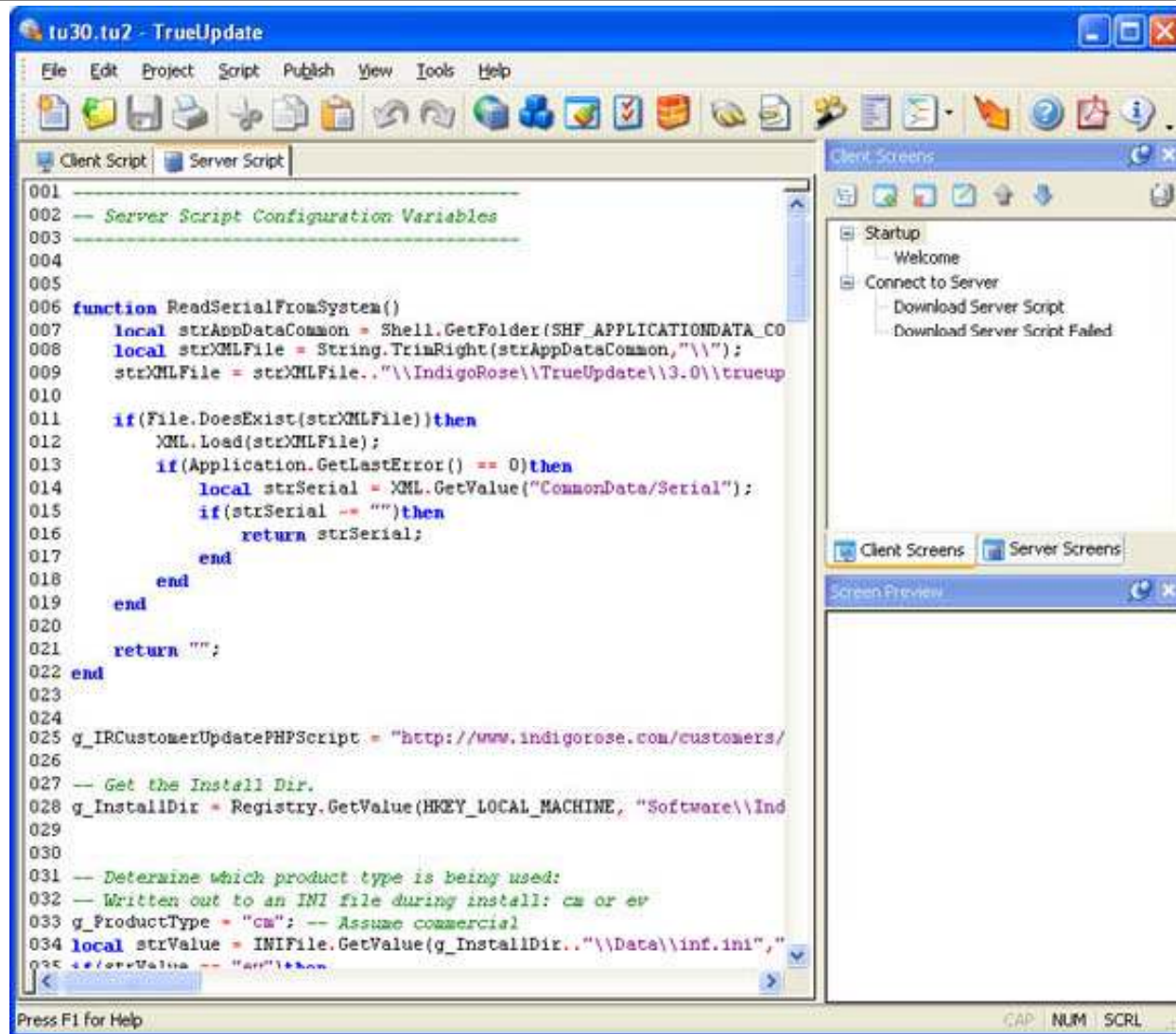
TrueUpdate: Screenshot 2



The screenshot displays the TrueUpdate application window titled "tu30.tu2 - TrueUpdate". The main area is a script editor showing a Lua script. The script includes comments for downloading and running server scripts, test mode settings, and a function to check for quiet updates. On the right side, there are two panels: "Client Screens" and "Screen Preview". The "Client Screens" panel shows a tree view with "Startup" (containing "Welcome") and "Connect to Server" (containing "Download Server Script" and "Download Server Script Failed"). The "Screen Preview" panel is currently empty.

```
01 -----
02 -- Download and run the Server Script
03 -----
04
05 -- Test mode - turned on by /TESTMODE command line argument.
06 -- This mode makes it try the 1 and 1 server first.
07 -- If running update tests, upload only to the 1 and 1 site
08 -- and pass the /TESTMODE cmd line arg.
09 g_IsTestMode = false;
10
11 local strArg = "";
12 local i = 0;
13 if(_CommandLineArgs)then
14     for i, strArg in _CommandLineArgs do
15         if(String.CompareNoCase(strArg, "/TESTMODE") == 0)then
16             g_IsTestMode = true;
17             Dialog.Message("Notice", "You are in test mode.");
18         end
19     end
20 end
21
22 -- Is it a quiet update (silent until update available)?
23 function IsQuietUpdate()
24     local bFound = false;
25     for i, arg in _CommandLineArgs do
26         if(arg == "/QUIET")then
27             bFound = true;
28         end
29     end
30     return bFound;
31 end
32
33 -- This will tell us:
34 g_IsQuietUpdate = IsQuietUpdate();
35
```

TrueUpdate: Screenshot 3



Tool: FlashUpdate

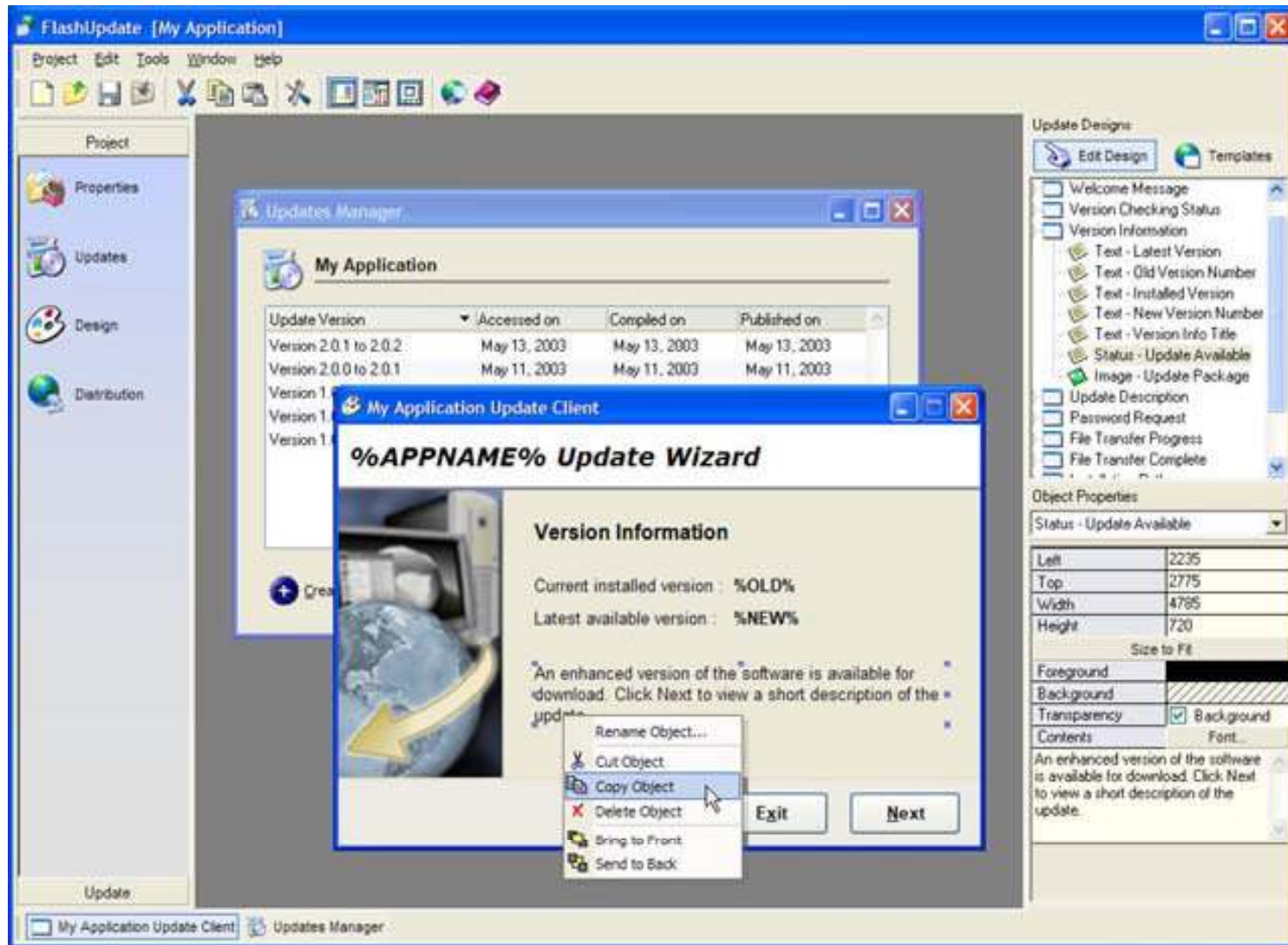
FlashUpdate is a software update solution for windows developers

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

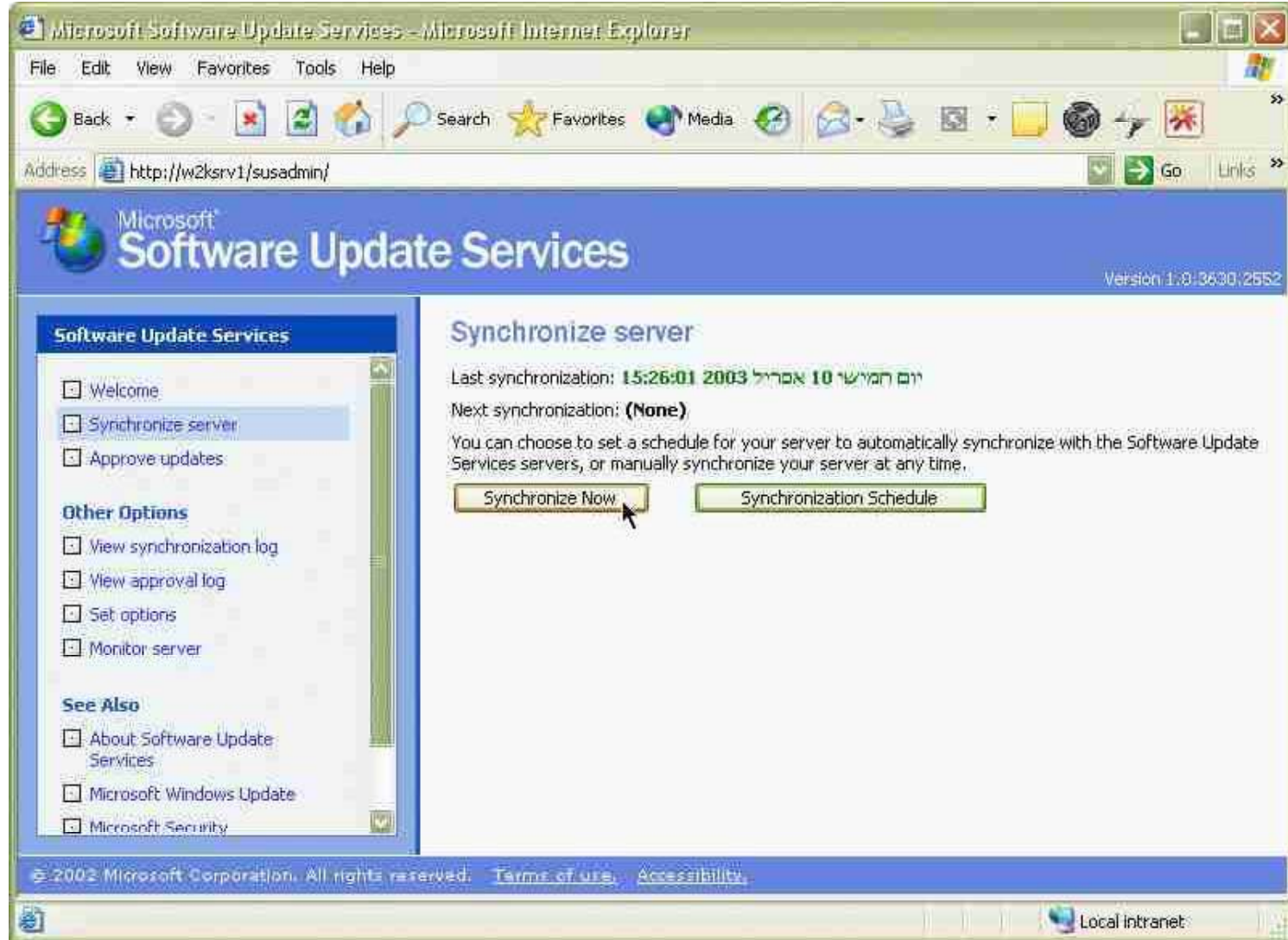
Administrators can receive e-mail notification when updates are added to their SUS pipeline

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

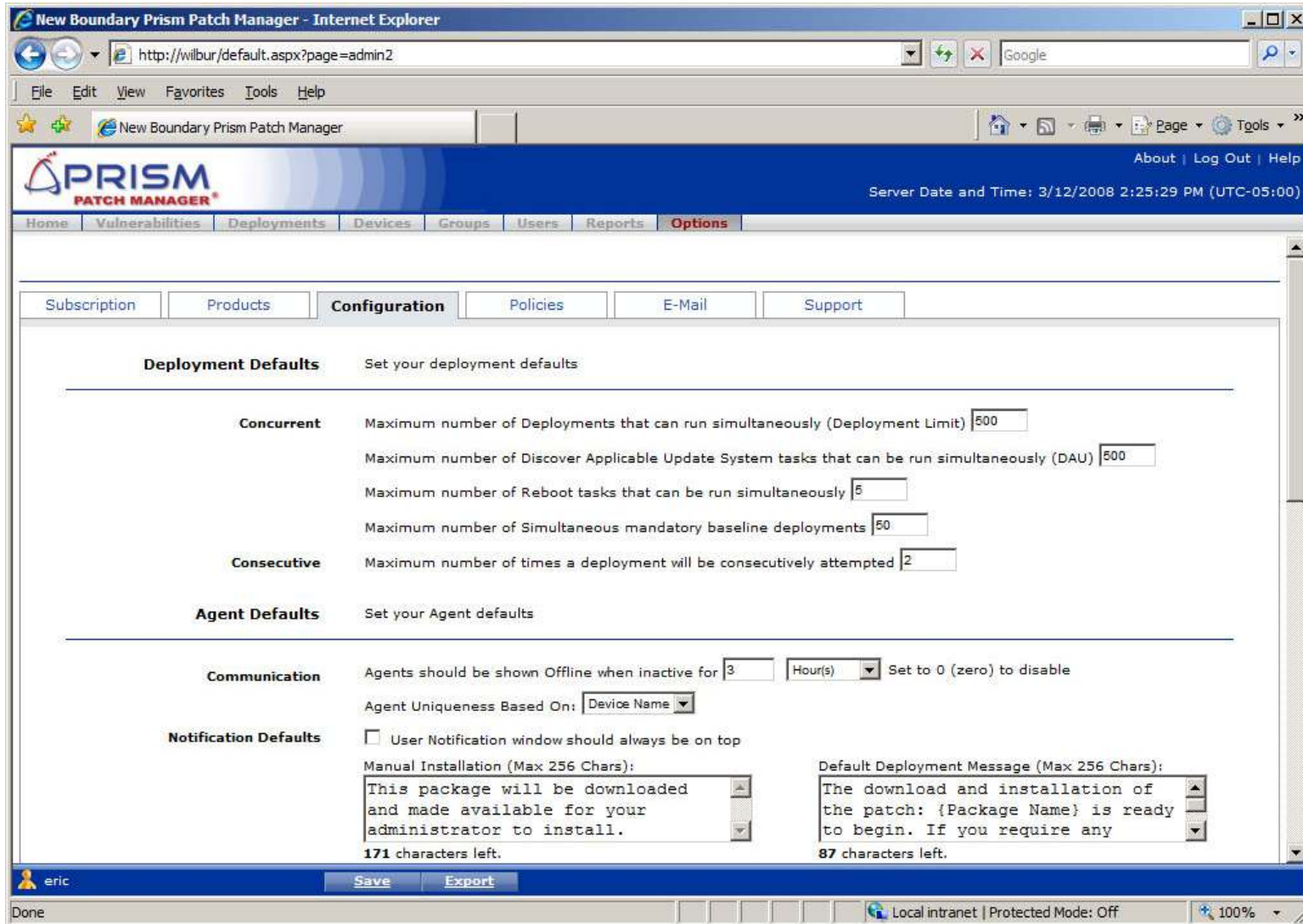
Vulnerabilities

Vulnerability Name	Impact	Progress
MS07-028 931906 Vulnerability in CAPICOM (SEE NOTES)	Critical - 01	100%
MS07-042 936227 936181 Vulnerability in Microsoft XML Core Services (MSXML4) (Rev 3)	Critical - 01	100%
MS06-061 924191 925672 925673 Vulnerabilities in Microsoft XML Core Services (MSXML4)	Critical - 05	100%
MS06-071 928088 927978 Vulnerability in Microsoft XML Core Services (MSXML4) (Rev 2)	Critical - 05	100%
Scan Report for WMF Vulnerability (912840) Third Party Temporary Workaround wmfhotfi...	Critical - 05	100%
MS 887606 Update for MSXML 2.0 SP6	Recommend	100%
MS 887606 Update for MSXML 4.0 SP2	Recommend	100%
MS 909520 Microsoft Base Smart Card Cryptographic Service Provider Package	Recommend	100%
MS 909915 Patch 1 for installing Australian Daylight Saving time zones for year 2006 (SE...	Recommend	100%
MS 932590 DST update to C Runtime Library msvcrt.dll for C applications	Recommend	100%
MS 941833 Update for Microsoft XML Core Services 4.0 Service Pack 2	Recommend	100%
Adobe Acrobat Reader 6.0	Software	100%
Adobe Acrobat Reader 6.0.1	Software	100%
Adobe Acrobat Reader 7.0.5	Software	100%
Adobe Acrobat Reader 7.0.7	Software	100%

Total: 114

eric | Deploy | Disable | Enable | Export | Update Cache | Scan Now

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

The screenshot displays the VisLogic Patch-Magic V3.0 interface. The left sidebar contains a 'Patch-Magic Systemmenü' with options like 'Netzwerk Übersicht', 'Computer sortiert', 'Vollständig up to date', 'Updates ausstehend', 'Reboot ausstehend', 'Malwareverseucht', 'Problemrechner', 'Unlizenzierte', 'Funktionen per Doppelklick', 'Ereignisprotokoll', 'Patchdatenbank', 'Einstellungen', 'Zeitplan', 'Anti Malware Einstellungen', 'Netzwerkeinstellungen', 'Sonstige Einstellungen', 'Spracheinstellungen', 'VisLogic Onlinedienste', and 'Sonstiges'. The main window shows a tree view of a 'Microsoft Windows-Netzwerk (9 von 50 lizenzierten Nodes)'. Under 'IP-Range', there is a 'Scan-Pool' containing nodes like 'VISLOGIC, Microsoft Windows 2000, Deutsch' and 'VISLOGIC2, Microsoft Windows 2000, Deutsch'. Below this, 'Malware Scanergebnisse' shows 'Status.....Keine Infektion gefunden.' and 'Letzter Scan...2008/03/17 12:17:24'. 'Wichtige Updates' lists several updates, including 'Bereits installierte' updates like 'Update-Rollup 1 für Windows 2000 SP4' and 'Windows 2000 Service Pack 4'. At the bottom, a table lists the nodes and their status.

PC Name	Platform	Gruppe	Status
VISLOGIC	Microsoft Windows 2000	IP-Range	ready.
VISLOGIC1	Microsoft Windows XP	IP-Range	ready.
VISLOGIC2	Microsoft Windows 2000	IP-Range	ready.
VISLOGIC3	Microsoft Windows XP	IP-Range	ready.
VISLOGIC4		IP-Range	ready.
VISLOGIC5		IP-Range	ready.
VISLOGIC_TEST1		IP-Range	ready.
VISLOGIC_TEST2	kein Admin / Scantimeout / Firewall	IP-Range	Scanprobleme
VISLOGIC_TEST3	Microsoft Windows XP	IP-Range	ready.

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

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