TotalCOMMAND Update 4.0 Comparison

Features	**TotalCOMMAND 4.0**	**HFNetChk Pro**
Built-in software distribution to install patches	YES	YES
Can calculate patch interdependencies and recommend only the patches you need based on the installed products and drivers	YES After selecting a patch, a list of computers that are applicable and meet the requirements for the specific patch is presented, so the user can quickly deploy the patch.	NO It is not aware of what software is installed on the system, it simply checks for OS patches.
Fully automatic disaster recovery	YES If the server crashes, simply create another server with the same DNS name and reinstall the TotalCOMMAND software with same serial number. All agents will connect and automatically repopulate the system.	NO Does not keep track of which patch is installed on which computer.
Can Inventory the client computers software and services	YES	NO
Enabled for mobile users	YES	NO
Can Inventory the client computers hardware	YES	NO
Automatic Notification to administrator if the patch was deleted or needs to be reapplied	YES	NO

TotalCOMMAND Update 4.0 Comparison

Features	**TotalCOMMAND 4.0**	**HFNetChk Pro**
Antivirus Enabled. Automatically updates all the definition and data files for major Antivirus companies	YES	NO
Hours of operation policies, which block any patch deployment during critical hours on specific servers or workstations	YES	NO
Source for Patch information	Multi-Source: TotalCOMMAND is the world's largest repository of automated patches and is the provider of its own patch XML content. It also monitors other vendors such as Microsoft, Intel, Symantec, McAfee and many others for XML content.	Single Source: Microsoft XML
Automatic Caching System (ACS). Auto caching security related patches and critical patches during the night for rapid deployment	YES	NO
Hardware profile locking to inform administrator when hardware inventory changes on a given computer	YES	NO
Service task locking to inform administrator when new services are added or removed on client computer	YES	NO
Patch Compliance Assurance Mechanism (PCAM™) Automatically installs patches that are removed or dropped as a result of user or backup/restore operation	YES	NO
Features	**TotalCOMMAND 4.0**	**HFNetChk Pro**

TotalCOMMAND Update 4.0 Comparison

Integrated Custom Patch builder	YES	NO
Support for all Windows family 95,98,ME, NT, 2K and XP	YES	No support for 95,98,ME
Administrator can create groups of computers for each department with its own view and management schemes	YES	NO
Administrator can define mandatory baseline patches to automatically install missing patches or software products	YES	NO
Reboot control over mandatory patches	YES	NO
Patches installed in a lab on a variety of configurations before release and signed by the testers with results of the test	YES	NO
Web-based user interface, the tool goes where the administrator goes	YES, simply open a browser and manage the patches and deployments.	NO
Administrator can select a specific group of computers to install the patches	YES	YES
Features	**TotalCOMMAND 4.0**	**HFNetChk Pro**
Administrator can select the date and time for the deployment of each patch	YES	???
Software and patch locking to inform administrator if any user installs or removes any software or patches	YES	YES

TotalCOMMAND Update 4.0 Comparison

All communication to the Internet is done over a highly secure 128-bit SSL connection to obtain original patches from host	YES	NO
Patches available for software vendors other than Microsoft such as; Adobe, IBM, Intel, 3Com, Novell, Corel, MacroMedia...	YES	NO
Uninstall bad or unwanted patches (Roll Back)	YES	YES
Automatic detection if patch has been tampered with and installation will not proceed	YES	NO
Patch compression during download over Internet to allow bandwidth conservation	YES	NO
Patch compression during deployment to workstations/servers	YES	NO
Chaining patches together, suppressing reboot	YES	YES
Features	**TotalCOMMAND 4.0**	**HFNetChk Pro**
Scan Method	Parallel, where each computer scans itself and reports the result to the server. This method is highly scalable and does not generate much network traffic.	Sequential
Will update computers outside the LAN and domain environment without any changes to the firewall	YES uses HTTP and HTTPS	???

TotalCOMMAND Update 4.0 Comparison

Scalability for enterprise level deployment by clustering patch servers	YES	NO
Agent policy, can automatically replicate to all agents with or without active directory or domain	YES	No agent policy support
Bandwidth throttling	YES	NO
Resumes patch download if the connection breaks	YES	NO
Patches can be cached at multiple physical locations using cache appliances for rapid deployment	YES	NO
Features	**TotalCOMMAND 4.0**	**HFNetChk Pro**
Managed internet access from the server. (When downloading patches for some applications, such as I.E., only the server will access the internet and pull down the patches) Clients do not have to have access to the internet	All clients receive their patches from the TotalCOMMAND Server and do not have to have internet access for security reasons.	NO
Automatically scan and notify the administrator when new patches arrive.	YES	NO

Agent Vs Agentless

Q1) What are the benefits of installing agents on my computers?

TotalCOMMAND Update uses advanced client-side agent technology to communicate with the TotalCOMMAND Update Server. The main reason for using agents is to increase performance and scalability of an enterprise-wide solution. Agents accelerate the performance of a large-scale deployment and a single enhanced Update Server can service literally tens of thousands of Web-based client agents. TotalCOMMAND Update agents can work across firewalls and operate on literally any computer that has a TCP/IP connection to the enterprise network.

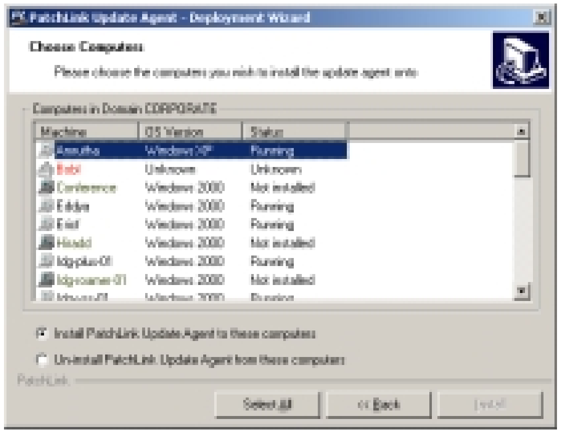
TotalCOMMAND Update 4.0 Comparison

1. Most major enterprise software management tools use agents, such as Microsoft SMS, Active Directory, IBM's Tivoli products, Symantec Anti-Virus, McAfee Anti-Virus and Novell Zen. In large networks, agents can “wake up” and report to the server when they have information to report in parallel. In comparison, tools that do not use agents must rely on remote API calls, which must be polled continuously from the server and can be extremely slow and not scalable in large environments.
2. Agents can receive compressed files to conserve bandwidth and, for increased security, also identify if the patch has been tampered with. An agent can resume a download when it is disconnected from a network and reconnect at different locations — a necessity for mobile users. Patch tools that lack an agent must download the entire service pack or file every time they are interrupted and rely on a permanent LAN connection to function. They also tend to generate spikes in bandwidth utilization as patches are deployed. TotalCOMMAND Update Server can be tuned to only allocate a given amount of bandwidth per agent connection to take advantage of bandwidth-throttling.
3. Patch tools that rely on a domain connection and do not have an agent rely on "Remote Registry" Service. This service provides registry information to a remote computer and may be a security risk in many organizations where client computers are on the Internet. It allows a remote computer to read the registry information of a client computer. TotalCOMMAND Update does not use this service due to security reasons. Also this service is not available on Windows 95, Windows 98, and Windows ME — which describes why patch tools without an agent cannot operate on these platforms. TotalCOMMAND Update covers the entire Windows family securely.

Q2) How easy is it to install Agents?

TotalCOMMAND Update has a deployment wizard which can deploy to an entire domain in one install. It simply displays all the computers in the domain and allows the administrator to select the one he/she wants to deploy to. Then with a click of the mouse the agent is deployed on all selected computers. Users can also use a list of comma delimited computers for deployment.

In addition, a command line only install is available that can be used within a network login script on older workstations that are not part of the domain.



PatchLink Update Agent - Deployment Wizard

Choose Computers

Please choose the computers you wish to install the update agent onto

Computers in Domain CORPORATE

Machine	OS Version	Status
Anuutha	Windows XP	Running
Babi	Unknown	Unknown
Conference	Windows 2000	Not installed
Eddie	Windows 2000	Running
Enid	Windows 2000	Running
Hnadd	Windows 2000	Not installed
ldg-plus-01	Windows 2000	Running
ldg-scanner-01	Windows 2000	Not installed
[illegible]	Windows 2000	Running

● Install PatchLink Update Agent to these computers

○ Un-install PatchLink Update Agent from these computers

Q3) When you say Agents can wake up and report information to the server what does that mean?

In a large network you do not want to continuously scan the network, some traditional enterprise management tools that do this have been known to cripple performance of the LAN if poorly tuned. So our agents have been designed to wake up and report if new software was installed or a configuration change has occurred.

This tends to reduce the overall network traffic tremendously. On the other hand products that do not have agents need to scan the entire network each and every time to see what patches are needed – and that can take a lot of bandwidth as well as a huge amount of time as each node is scanned over the network by a central CPU. TotalCOMMAND Update behaves similar to like Anti-Virus products, users can scan his/her computer by simply going to the control panel and initiate a local scan to make sure things are patched and secure. Again, on software products without agents the user has no access to initiate a scan for his/her computer.

Q4) I already own a software distribution application, can I still use TotalCOMMAND Update?

Yes, TotalCOMMAND Update complements software distributions products. The software distribution tools are best for deployment but they can not accurately report the patch components that are installed on individual computers and therefore unable to calculate patch interdependencies and make patch recommendation.
The big issue with the traditional software distribution tools is that it needs lots of packages to build for every patch and that could need a small army of people to actually build and test the packages of software that are to be sent out. There is also nothing proactive about these solutions.
The IT staff is still fully responsible for going out and scanning the latest patch bulletins from the various manufacturers in order to figure out which patches you need.

With TotalCOMMAND Update, the story is completely different. TotalCOMMAND Update is a turnkey solution designed to be plugged into your network and then scan for the inventory configuration and patch levels on all workstations and servers within your network. Once the Update Server has done its job, the IT manager can then see a high level view of the entire connected Extranet - and see which patches need to go where.

The need for testing patches in the Administrator’s environment is significantly reduced since the TotalCOMMAND Update Subscription automatically delivers the latest patches and fixes ready for distribution within your environment. Best of all, the system intelligently recommends the most critical patches as they become available - not when your IT staff finally gets around to reading the latest security bulletins!

So even if an organization has an existing software distribution or software imaging solution in place, they need to add up the labor cost of patching their network effectively - or the potential damage of NOT patching - in order to realize the true return on investment with the TotalCOMMAND Update solution. Given the frequency with which new critical severity patches and updates appear, the average company can easily justify the cost of the TotalCOMMAND Update compared to the time and effort required to constantly re-image or manually distribute the fixes daily. Also with TotalCOMMAND Update companies can use their enterprise imaging / software distribution tools for major rollouts of new OS versions and application suites while using TotalCOMMAND Update for day-to-day patch maintenance.

Q5) Do I have to configure my Active directory, Domain or NDS to work with TotalCOMMAND Update?

Absolutely not. TotalCOMMAND Update is designed to work in heterogeneous environments, so it does not depend on any single directory or domain system. You can literally patch and update ANY computer that has a TCP/IP connection to your TotalCOMMAND Update Server whether across the LAN, WAN, VPN, dial-up, wireless

TotalCOMMAND Update 4.0 Comparison

Internet or any other network connections you may be using. TotalCOMMAND Update is the only VENDOR NEUTRAL solution to patching your entire network and will soon be offering agents across the LINUX/UNIX and NetWare operating systems to complement the Windows centric solution seen today. No other patching system can offer this flexibility – because no other solution is built purely on open, Internet protocols!