

# FrontRange DSM Patch Management™

## Improved Security and Cost Effectiveness Through Transparent Patch Management

Attacks in the form of hacking and malware occur on a daily basis and can lead to considerable economical damage for a company. Even unsuccessful break-in attempts can often cause critical systems and applications to malfunction or overload given bandwidths, resulting in a complete system shutdown. The offenders focus on targeting well-known weak points of operating systems and applications. According to key security experts between 50 and 60 such security vulnerabilities are discovered each week.

In order to protect against potential harm in the most efficient and cost-effective way possible, companies need a centralized, automated and constantly updated patch management solution. Before the patch is installed, it needs to be determined if it is relevant for the company and whether any dependencies or incompatibilities exist. A clear picture of the security issues and reliable proof of security compliance are imperative to satisfy internal and legal demands – even in complex and shared networks. However, this entire process must not slow down the response time, as speed is of the essence when installing new patches.

### Automated Security Scan and Patch Download

FrontRange Desktop & Server Management automatically scans the entire software environment for weak points, so that IT administrators always have an overview of the threat situation.

FrontRange DSM Patch Management™ lets you see all new patches from Microsoft at a glimpse and checks if changes were made to already released patches.

FrontRange DSM Patch Management enables you to select the necessary patches either from a local WSUS server or directly from the Microsoft Update website. The patch can be selected based on priority and the operating systems, service packs, applications and language selection programs actually installed in the company network. An info text provides you with information on troubleshooting as well as the direct link to the Microsoft Knowledge Base.

### Rule-Based Installation

FrontRange DSM Patch Management supports individual policy definitions for downloading and installing patches, so that entire processes can be fully automated and tailored to the company's needs. This also includes a scheduled download of Microsoft patches, thus deferring data transfers to specific times. Rule-based patch management with FrontRange Desktop & Server Management also relieves IT administrators of tedious tasks by allowing them to set one desired status without having to interfere manually.

This means, for instance, that all critical Windows 7 patches are first of all distributed automatically to all notebooks. The graphical user interface immediately indicates whether the defined status was achieved or not. If necessary, discrepancies can be tracked down all the way to the individual system. IT administrators thus are kept well informed of security compliance and any possible weak points, while the system documents the status for auditing purposes.



### KEY BENEFITS

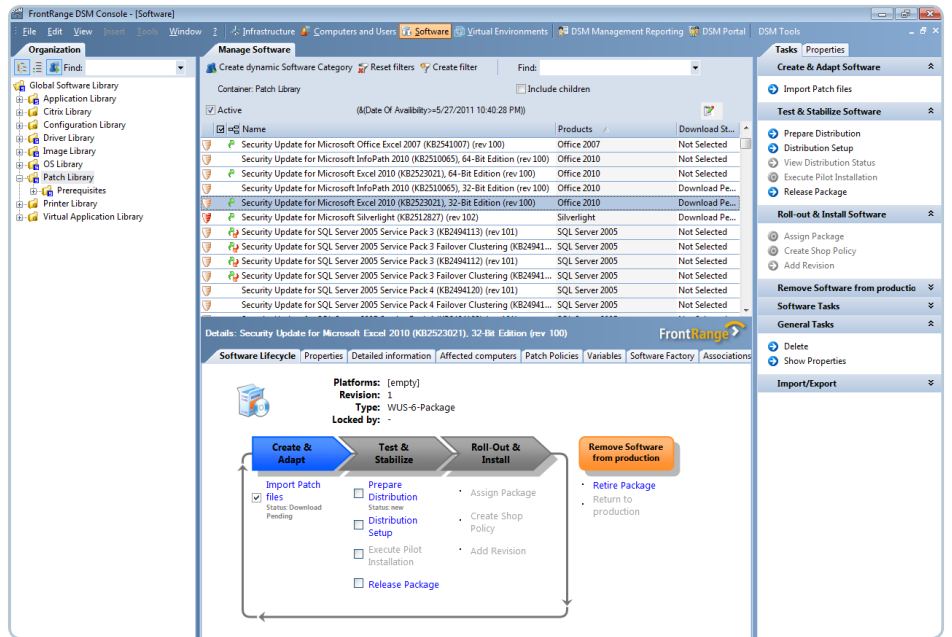
- Automation of all patch management stages
- Enhanced security thanks to automatic detection of weak points
- Reliable, rule-based rollout
- Quicker reaction to threats
- Flexible customization
- Reduced effort due to selection & automatic download of relevant patches
- Integrated quality control ensures higher stability
- Improved efficiency through seamless integration in FrontRange Desktop & Server Management.

### KEY FEATURES

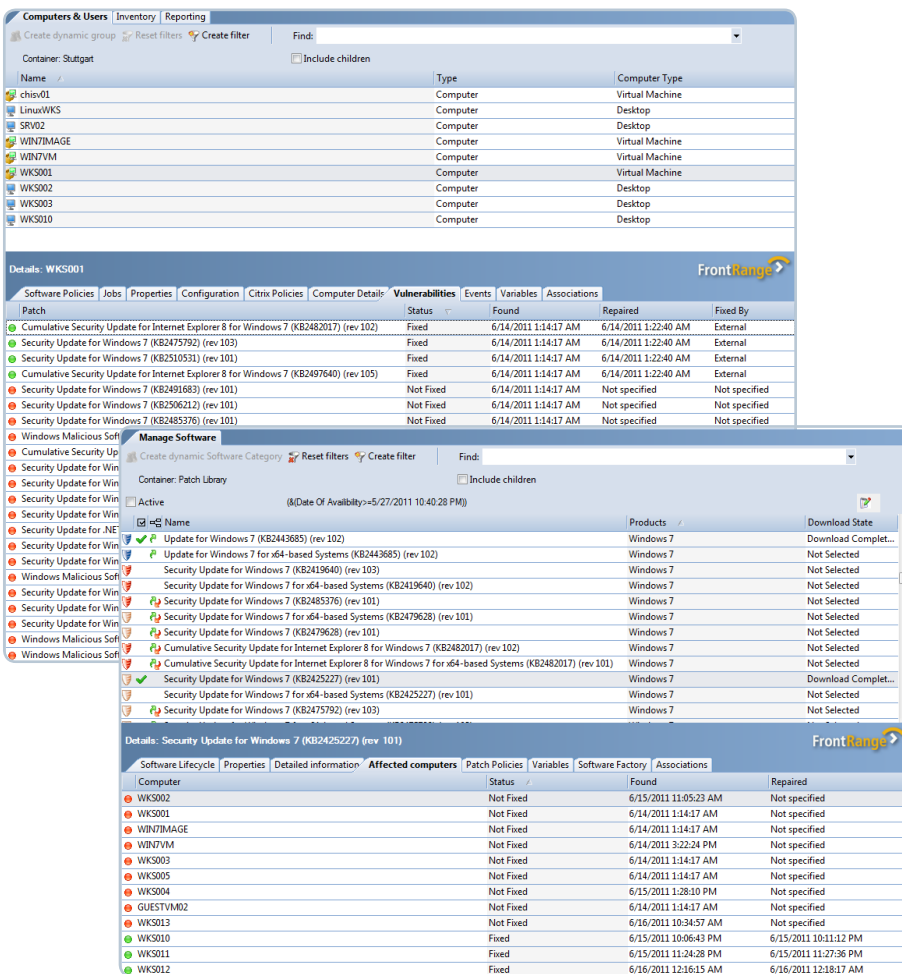
- Extensive selection of security patches for Microsoft applications and operating systems
- Timed patch catalog synchronization
- Timed patch download
- MBSA/WSUS patch catalog
- Installation via Windows Update Agent (WUA)
- Support of patch revisions
- Display and automatic resolving of patch dependencies
- Automatic identification of incompatibilities
- Vulnerability reports (security state)

**Pilot Installation Minimizes Risks**

Despite the urgency when installing patches, system stability and availability remain paramount. FrontRange DSM Patch Management supports controlled change management, whereby all new patches have to prove their harmlessness by being first tested in a pilot installation. FrontRange Desktop & Server Management only installs a patch on productive PCs if it passes these tests. FrontRange DSM Patch Management automatically resolves patch dependencies, thus minimizing the number of installations necessary.



Packaging Workbench for standardized and consistent patch processes



**SYSTEM REQUIREMENTS**

For a complete list of system requirements please refer to [www.frontrange.com/itam/system-requirements](http://www.frontrange.com/itam/system-requirements)

**MORE INFORMATION**

**Corporate Headquarters**  
 FrontRange Solutions USA Inc.  
 5675 Gibraltar Drive,  
 Pleasanton, CA 94588  
 USA  
 Tel: 800.776.7889  
 and +1 925 398 1800  
[www.frontrange.com](http://www.frontrange.com)

Clear representation of potential vulnerabilities and transparent compliance views