



RKA Petroleum

RKA Petroleum Companies Uses PatchLink Update™ to Halt Future Disasters

During 2003, RKA Petroleum Companies of Romulous, Michigan, faced the problem of the faulty patch. This petroleum products wholesaler had been struggling for months to keep current with the constant release of software patches from Microsoft and other vendors.

Things came to a head earlier this year when a critical server crashed because it was using the wrong software patch; IT staffers spent 15 hours on the phone with Microsoft reps trying to figure out which patch to deploy. Ultimately they ended up rebuilding the server.

“The problem was Microsoft assigned a patch that was not needed for the machine. There wasn’t enough disk space for the patch, and it started deleting files. Services started to fail, and people couldn’t log on to our network,” says Jason Hittleman, vice president of information systems at RKA.

“ Before this problem, we put all of our trust in Microsoft.
This opened our eyes to the issue. ”

Jason Hittleman - VP of Information Systems

Soon after the incident, RKA bought PatchLink Update™. RKA now uses the software to automatically deploy patches to its PCs and servers after approval by a human administrator.

The problem could have been avoided if the software had been in place to deploy the correct patch, Hittleman says.

“Before this problem, we had put all our trust in Microsoft. Whenever they recommended a patch, we wouldn’t think twice about it. This opened our eyes to the issue.”

Disasters of this nature highlight the importance of a rigid and structured patch management policy. Likewise, the problem faced by RKA illustrates that not all patches are created equal. RKA needed a solution to organize patch management to prevent future disasters from occurring.

Moreover, as a small company, RKA lacked many of the resources necessary to test patches before they are deployed, thereby forcing IT staff to deploy patches in a live environment.

According to Hittleman, the PatchLink Update™ software has already paid for itself in reduced labor costs.



KEY FACTS:

- Small company without the necessary resources for patch testing
- Patches deployed into a live environment
- Improper patch assigned to server by Microsoft
- Files deleted and critical services failed
- IT staff unable to restore system