ATOMICdata

SERVER & WORKSTATION

PATCH MANAGEMENT

You've seen it before, you may have even been a culprit—systems left unpatched for weeks, months, or even years. But slow or no patching is one of your biggest security risks. With Atomic Data's Patch Management you'll get single source views of your systems, with automated patching schedules to cut down on the time it takes to patch.

- Weekly & biweekly scans of each device for new patches
- Engineers test & whitelist patches
- Patches implemented after approval
- Engineers on-call to remediate issues post-patching
- Custom patching schedules available
- Monthly reporting available

60%
Percentage of breaches resulting from unpatched vulnerabilities

Unpatched systems make ideal targets for malicious actors to gain unfettered access to your systems and confidential data. Each new patch represents a vulnerability — an unlocked window into your systems. Fast, automated patching is your best defense.

Microsoft

Microsoft Windows

Atomic Data utilizes Kaseya Virtual System Administrator (VSA) to perform patch management activities on Windows devices. A lightweight agent is installed on each monitored endpoint. Once updates are identified and white listed by Engineers, the patch is automatically pushed to the machine according to pre-defined patching windows. Based on your needs we can develop custom schedules, provide reporting, and patch additional software.

Linux

Linux Patch Management maintains security and reduces labor costs via frequent and automated software patching. Engineers install an agent on each managed server and configure the patching schedule within the management server. The lightweight agent periodically checks-in with the central management system to determine patch status and find new applicable patches. Patches are then applied during a pre-defined two hour window or a customized window, depending on your business needs.