



BARAMUNDI CHECKLISTS provide concise, step-by-step expert advice for handling common IT challenges in a straightforward way. You can find more checklists at: www.baramundi.com/checklists

Efficient and reliable Windows update and patch management

The pressure to keep up with Windows updates and third-party software patches continues to grow along with the number of and types of vulnerabilities affecting them. That makes update and patch management an increasingly important – and time-consuming -- IT responsibility. We recommend the following structured approach to keep up with updates and patches efficiently:

✓ Identify critical hardware and software

Continuously assess current risks beginning with mission-critical systems and software applications that are essential for maintaining productivity in different departments. Prioritize patch and update deployments accordingly.

✓ Pre-deployment testing

Updates and patches can contain bugs or introduce unexpected incompatibilities. Test patches and updates on representative devices and configurations first to spot and correct problems before wider deployment. This will minimize endpoint crashes and slowdowns.

✓ Implement deployment rings

Create rings of endpoints or logical groups of devices that will receive applicable updates at the same time in a step-wise sequence of increasingly larger rings. The rings with the most important endpoints will receive patches or updates first.

✓ Automate!

Updating manually is time- and labor-intensive as well as prone to errors. The key is automation. Patch and update rollouts can be configured in detail and deployed. Advanced UEM solutions also provide extensive libraries of pre-tested patch packages ready to be distributed.

✓ Manage and isolate risks

Not all updates and patches can or should be deployed immediately. Apart from buggy or incompatible updates, there are legacy systems that cannot easily be changed, especially those used in real-time production environments. It may be necessary to isolate or disconnect or secure them with other measures.

This structured approach can help IT teams deploy needed patches and updates efficiently, promptly and reliably to optimize endpoint performance, network security and user productivity. The **baramundi Management Suite (bMS)** modules Inventory, Network Devices, Vulnerability Scanner, Update Management, Deploy and Automate as well as Managed Software provide all capabilities needed for the best possible network protection.

ALL ENDPOINTS UNDER CONTROL

The baramundi Management Suite empowers IT teams with the tools and flexibility needed for managing today's hybrid computing environments from any location. Learn more about Unified Endpoint Management with baramundi at www.baramundi.com.