

Managing Windows Updates with AI:

Optimizing Monitoring, Approval, and Reboot Handling



Efficient management of Windows updates is critical to maintaining security, performance, and compliance across enterprise environments. As organizations face an increasing volume of updates, integrating AI into update management can help streamline processes, enhance decision-making, and minimize disruptions. While AI does not fully automate every task, it plays a crucial role in monitoring, approving, and handling reboots. By leveraging tools like Microsoft's Windows Autopatch with Copilot, NinjaOne, and Infraon Assets, businesses can improve their update management strategies and reduce the time and effort required to resolve issues.

1. Using Microsoft Windows Autopatch with Copilot AI

Windows Autopatch is a cloud-based service designed to automate the deployment of updates for Windows devices. It integrates AI through Microsoft Intune's Copilot to enhance the monitoring and approval process. The service manages monthly quality updates, feature updates, and drivers, with AI providing intelligent insights for troubleshooting and remediation. One standout feature is hotpatching, which allows for applying security updates without requiring device reboots in many cases.

Steps for Setup and Management:



Prerequisites:

Devices must be enrolled in Microsoft Intune and meet the requirements for Windows Autopatch (e.g., Windows 11 Enterprise). The service is enabled via the Intune admin center under Devices > Windows > Windows Autopatch.



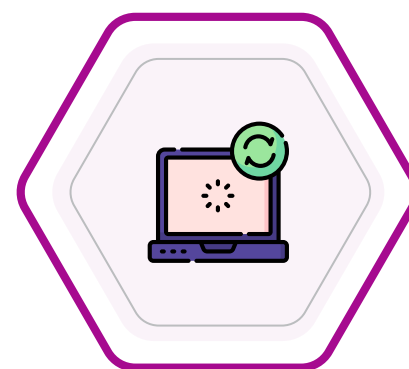
Monitoring with AI:

In the Intune admin center, navigate to Windows Updates and select "Explore with Copilot." AI supports query-based insights, such as identifying devices without the latest quality updates or proposing remediation for outdated devices.



Approval with AI:

Cloud-based policies allow for both automatic and manual approvals. AI analyzes risks associated with each update, flagging potentially risky updates, such as those for devices nearing end-of-support.



Reboot Handling:

Hotpatching ensures that security updates can be applied without reboots. Scheduled maintenance windows and AI-driven queries, like "Which devices need a reboot after updates?", help manage reboots efficiently.



Best Practices:

Start with a pilot group of devices and scale gradually.



Rate Copilot's responses to improve future decision-making.



Integrate with Intune's update rings for more granular control over deferrals, such as delaying feature updates for up to 365 days.

By integrating AI, Windows Autopatch reduces manual oversight and accelerates the resolution of update-related issues, enhancing overall update management.

2. Using NinjaOne with Patch Intelligence AI

NinjaOne is an endpoint management platform that automates patching across multiple operating systems, including Windows, macOS, and Linux. Its Patch Intelligence AI uses sentiment analysis and global user feedback to identify potentially problematic patches, offering intelligent insights for safer patch approval and deployment.

Steps for Setup and Management:



Prerequisites:

Sign up for NinjaOne, install agents on target devices, and configure patching policies under Patch Management.



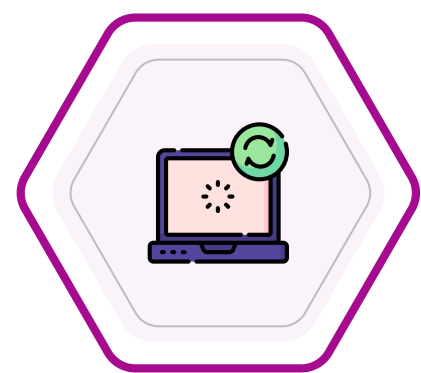
Monitoring with AI:

AI-enabled policies scan for patches with known issues (e.g., stability problems) based on community feedback. The system provides real-time visibility into patch status and surfaces alerts for high-risk patches.



Approval with AI:

Set policies to auto-approve security updates, with AI suggesting overrides for patches flagged with negative sentiment (e.g., known compatibility issues). A combination of auto-approval and manual review ensures a balanced approach.



Reboot Handling:

NinjaOne allows for automatic reboots post-installation or during scheduled maintenance windows. AI helps prevent issues like boot loops or unintended reboots by avoiding unstable patches.



Best Practices:

Deploy updates in phases (e.g., from pilot to production).



Use audit reports to monitor compliance and AI to ensure that only vetted patches are applied.

By utilizing Patch Intelligence AI, NinjaOne enhances proactive risk mitigation, making it an ideal solution for Managed Service Providers (MSPs) handling diverse environments.

3. Using Infraon Assets for AI-Powered Patch Management

Infraon Assets offers AI-driven patch management for Windows updates across endpoints, servers, and remote devices. This solution provides real-time monitoring and predictive risk analysis, assisting IT teams in prioritizing updates and managing patches efficiently.

Steps for Setup and Management:



Prerequisites:

Install Infraon Assets, discover devices, and set up patch groups based on your network.



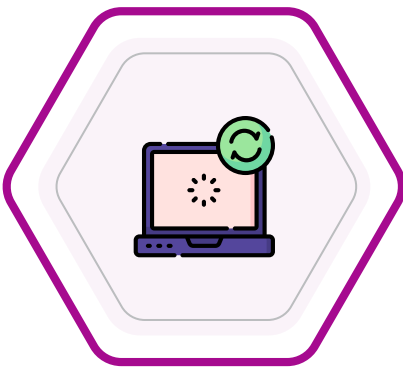
Monitoring with AI:

AI-powered dashboards display real-time patch status (e.g., pending, approved, or completed), with AI analyzing vulnerabilities and prioritizing high-risk patches.



Approval with AI:

AI supports policy-driven workflows that assist with patch approval based on risk analysis. Patches are staged for testing before full rollout, ensuring better compliance and security.



Reboot Handling:

Policies allow you to define reboot schedules and maintenance windows. Automated rollbacks can be triggered if issues arise post-reboot, with AI facilitating rapid issue resolution.

Best Practices:

Align patch management with organizational policies for timing.



Use audit reports to track update status and ensure centralized updates to prevent fragmentation.

Infraon Assets excels in providing comprehensive patch management with AI, offering high efficiency and policy enforcement for organizations.



General Best Practices Across Tools

01. Automation Integration:

Leverage tools like PowerShell or Intune for baseline automation, while allowing AI to handle smart decisions such as override approvals for risky patches.



02. Security and Compliance:

Always test patches in pilot environments before full deployment, monitor for failures, and ensure that updates come from trusted sources (e.g., via WSUS integration).



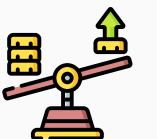
03. Minimizing Disruptions:

Prioritize hotpatching or off-hours reboots to reduce downtime. AI can predict the impact of reboots by analyzing historical update data.



04. Scaling:

Start small by rolling out patches to a limited set of devices, monitor metrics like success rates, and refine policies based on insights provided by AI.



Conclusion

AI-powered tools like Microsoft Windows Autopatch with Copilot, NinjaOne, and Infraon Assets are transforming how businesses manage Windows updates. These tools not only automate essential tasks but also provide intelligent insights that enhance decision-making processes, minimize manual intervention, and reduce downtime caused by disruptive updates. By integrating AI, organizations can ensure timely, secure, and efficient updates while managing compliance and reducing risks.

