Action1
patching that works

15 Essential Automations for Effective Patch Management

Discover key 15 automations for improving patch management efficiency. Covering everything from vulnerability assessment to compliance reporting and rollback capabilities, it provides straightforward advice on automating critical patch management functions to enhance security and compliance while reducing manual workload.

1. Vulnerability Scanning and Assessment Automation: Automatically assess systems and applications for vulnerabilities on a regular basis to identify which patches are needed, prioritizing based on severity.

2. Patch Availability Monitoring: Set up automation to continuously monitor for new patches and updates from software vendors and security bulletins to ensure you are always aware of the latest updates.

3. Automated Patch Testing: Before deploying patches widely, automatically apply them in a controlled testing environment to check for compatibility issues, software conflicts, or disruptions.

4. Prioritization and Scheduling: Automate the prioritization of patches based on the severity of the vulnerabilities they address and schedule patches for off-peak hours to minimize business impact.

5. Patch Deployment Automation: Implement systems that automatically deploy patches to targeted devices and systems, ensuring that critical security patches are applied as soon as possible.

6. Compliance Checks and Reporting: Regularly automate compliance checks to ensure that all systems are up-to-date with the required patches and generate reports for audit and compliance purposes.

7. Rollback Capabilities: Set up automation to quickly rollback patches that cause issues, minimizing downtime and maintaining system stability.

8. Endpoint Configuration Management: Automatically manage and enforce policies for endpoint configurations to ensure they meet security standards and are compliant with patch management policies.

9. Automated Notifications and Alerts: Configure alerts to notify IT staff about critical vulnerabilities, failed patch deployments, and systems that are non-compliant with patch management policies.

10. Integration with ITSM Tools: Automate the integration of patch management processes with IT Service Management (ITSM) tools to streamline ticketing, incident management, and change management related to patching activities.

11. User Communication Automation: Set up automated communications to inform users about upcoming patches, particularly for devices that require a reboot or user intervention. This ensures users are prepared and can save their work to prevent data loss during the patching process.

12. Automated Remediation for Failed Patches: Implement systems that automatically attempt to remediate failed patch installations. This could involve retrying the installation, clearing cache files that might be causing the issue, or resetting services that are essential for the patch process.

13. Custom Patching Scripts Automation: For complex applications or systems that require specific patching procedures, develop and automate custom scripts that tailor the patch deployment process to meet unique requirements, ensuring consistency and reducing manual intervention.

14. Security Policy Enforcement: Automate the enforcement of security policies that require certain patches to be installed as a condition of network access. This can include automatically quarantining non-compliant devices until they are updated.

15. Automated Inventory and Asset Management: Continuously update your IT asset inventory with automated discovery tools to ensure all devices, including mobile and IoT devices, are accounted for in the patch management process. This helps to avoid blind spots in the security posture and ensures that no device is left vulnerable.

Automating Patch Management with Action1

With Action1, you can automate the entire patch management process of numerous software and OS titles with real-time progress status, from identifying and deploying missing updates to compliance reporting, even if your endpoints are offline.

Action1 reinvents patch management with an infinitely scalable and highly secure platform configurable in 5 minutes that just works. With integrated real-time vulnerability discovery and automated remediation for both third-party software and OS, peer-to-peer patch distribution, and IT ecosystem integrations, it ensures continuous patch compliance and reduces security and ransomware risks – all while lowering costs. Action1 is certified for SOC 2/ISO 27001 and is trusted by thousands of enterprises managing millions of endpoints globally.