Action1
#1 for patch management

Third-Party Patching Playbook: 16 Expert Tips

As businesses rely more on software tools, efficient third-party patch management is crucial. This document offers practical tips and strategies to automate vulnerability detection and remediation in third-party applications. From prioritizing applications to utilizing expert tools and best practices, this guide helps you fortify your network, reduce risks, and streamline patch management while maintaining compliance with industry standards.

1. **Apply a Risk-Based Patch Management Approach to Your Software:** Identify and prioritize critical software applications, such as web browsers and office suites, because these are the most appealing targets for cyberattacks due to their widespread usage and vulnerabilities.

2. **Harness Automation for Effortless Patch Management:** Choose patch management tools that support third-party applications to ensure a comprehensive approach to patching, and enable automation to streamline the scanning, downloading, and scheduling of patches, reducing the need for manual intervention.

3. **Opt for Centralized Control:** Implement a centralized patch management solution that offers a single dashboard for monitoring and managing patches across multiple applications, enhancing efficiency and control.

4. **Prioritize Patching Based on Vulnerability Severity:** Utilize vulnerability scanning tools to identify weaknesses in your network and prioritize patching based on the severity of vulnerabilities.

5. **Ensure Patch Compatibility Through Controlled Testing:** Test patches in controlled environments to ensure they won't disrupt critical operations or conflict with other software, and always have a rollback plan in place to quickly revert to the previous system state if issues arise, minimizing downtime.

6. **Minimize Disruptions with Smart Patch Scheduling:** Schedule patch deployments during low-traffic hours or non-business hours to minimize disruptions to productivity, and educate employees about the importance of prompt patching to reduce security risks associated with delayed updates.

7. **Enforce Clear Patch Management Policies and Monitoring:** Develop clear patch management policies and procedures that outline the roles and responsibilities of IT staff and end-users in the patch management process, and continuously monitor patch status while generating reports to track compliance and vulnerabilities.

8. **Stay Compliant and Invest in Ongoing Training:** Ensure compliance with relevant industry regulations and standards, such as GDPR, HIPAA, or PCI DSS, if applicable to your organization, and invest in training for IT staff to keep them updated on the latest patch management best practices and tools.

9. Automate Updates for Non-Critical Software: Encourage users to enable auto-updates for non-critical software applications to ensure they are kept up to date without manual intervention, and subscribe to vulnerability databases and mailing lists to stay informed about the latest security threats and patches.

10. Adapt and Improve with Regular Process Review: Periodically review and adapt the patch management process to identify areas for improvement, adapt to changes in the threat landscape, and incorporate emerging best practices to enhance overall security.

11. Customize Patch Testing and Establish Baselines: Focus your testing efforts on critical applications and systems to prioritize what matters most to your organization, and establish patch baselines to maintain consistency in managing software updates.

12. Efficiently Address Vulnerabilities with Automation and Phases: Opt for a solution that integrates vulnerability scanning seamlessly into your patch management process. This ensures swift vulnerability identification and patch deployment, while controlled phased deployment ensurees issue identification before a full rollout.

13. Prepare for Issues with Automated Rollback and Integration: Consider implementing automated rollback procedures within your patch management solution to save time and reduce the potential for human error when reverting to a previous system state, and integrate patch management with your organization's change management procedures to ensure alignment and documentation.

14. Leverage Threat Intelligence and User Feedback: Incorporate threat intelligence feeds into your patch management process to make informed decisions regarding patch prioritization based on real-time threat information, and establish user feedback channels to quickly address any unforeseen problems or issues reported by end-users.

15. Maintain Accurate Asset Records and Consider Custom Automation: Maintain an up-to-date asset inventory to track all hardware and software across your organization, ensuring that critical systems are not overlooked during patching efforts, and consider creating custom patch automation scripts for advanced users to tailor patching tasks to specific organizational needs.

16. Measure Performance Metrics and Maintain a Documentation Repository: Define key performance indicators (KPIs) and metrics to measure the effectiveness of your patch management process, regularly review these metrics to identify areas for improvement, and maintain a comprehensive patch documentation repository that includes release notes, installation instructions, and known issues to aid in troubleshooting and reference.

Easy and Powerful Third-Party Patching with Action1

Automate vulnerability detection and remediation in third-party applications with Action1. The Vulnerabilities dashboard provides a centralized view of network vulnerabilities, while the Action1 App Store offers a secure repository of 150+ third-party apps, including the ability to upload custom software packages. Action1 is the only third-party patch management solution with both SOC 2 Type II and ISO 27001:2022 certifications.