Action1
#1 for patch management

Compliance 101: Roadmap in 10 Steps

In today's fast-paced digital landscape, ensuring security and regulatory compliance is paramount. This guide simplifies the complex world of patch management compliance. Whether you're already well on your way to compliance or are just beginning the journey, this guide provides a clear and concise breakdown of the essential steps. It serves as a valuable resource to help you identify your starting point and navigate the path forward.

1. **Identify Applicable Regulations:** Understand the specific patch management requirements set by the regulations relevant to your industry, such as PCI DSS, HIPAA, SOC 2, CIS CSC, ACSC Essential Eight, GLBA/FFIEC, etc.

2. **Establish Patch Management Policy:** Develop a comprehensive patch management policy that aligns with the requirements of the applicable regulations. This policy should define roles and responsibilities, patch deployment procedures, timelines, and exceptions.

3. **Perform Risk Assessment:** Conduct a risk assessment to identify critical systems, applications, and assets that require patch management. Prioritize based on the potential impact of vulnerabilities and their exploitation.

4. **Monitor and Track Vulnerabilities:** Stay informed about new vulnerabilities by monitoring security advisories, alerts, and vendor notifications. Leverage vulnerability management tools and services to assess your systems for vulnerabilities and track their remediation status.

5. **Patch Testing and Validation:** Establish a process for testing patches in a controlled environment before deploying them in production. Validate that patches do not negatively impact system functionality, stability, or compatibility with other applications.

6. **Patch Deployment and Timelines:** Implement a regular and timely patch deployment process. Define appropriate timelines for patch installation based on the severity and criticality of vulnerabilities, as mandated by the regulations.

7. **Patch Management Tools:** Utilize automated patch management tools to streamline the identification, deployment, and reporting of patches. These tools can assist in vulnerability scanning, patch inventory management, and tracking patch compliance.

8. Documentation and Auditing: Maintain comprehensive documentation of patch management activities, including patching schedules, installation records, testing results, and any exceptions or deviations from standard procedures. Conduct regular audits to ensure adherence to patch management policies and regulatory requirements.

9. Employee Awareness and Training: Educate employees on the importance of patch management, the role they play in maintaining a secure environment, and the potential risks associated with unpatched systems. Provide training on recognizing phishing emails and social engineering attempts that could exploit unpatched vulnerabilities.

10. Ongoing Monitoring and Review: Continuously monitor the effectiveness of your patch management program. Conduct periodic reviews and assessments to evaluate the adequacy of your patch management processes, identify areas for improvement, and ensure compliance with evolving regulations.

Continuous Patch Compliance with Action1

Action1 is the #1 risk-based patch management platform for distributed enterprise networks trusted by thousands of organizations globally. Action1 helps to discover, prioritize, and remediate vulnerabilities in a single solution to prevent security breaches and ransomware attacks. It automates patching of third-party software and operating systems, ensuring continuous patch compliance and remediation of security vulnerabilities before they are exploited.

Automate some of the most tedious patch compliance activities to reduce risk to your environment and data, pass compliance audits faster and with a better compliance rate, and free up your time for other strategically important IT projects. Explore what patch compliance activities you can streamline with Action1, the first vendor focusing on patch management to achieve both ISO 27001:2022 and SOC 2 Type II:

- Discover, prioritize and remediate vulnerabilities
- Ensure continuous patch compliance for servers and workstations
- Automate patch management for OS and third-party apps
- Maintain up-to-date inventory