# The rise of automated patch management in cybersecurity



The increasing frequency and sophistication of cyber attacks is driving companies to adopt automated patch management systems, in light of projections from an International Monetary Fund report which estimates the global cost of cyber crime could rise to $23 trillion by 2027—a staggering increase of 175% from 2022. This escalation in cyber threats has underscored the necessity for rapid and effective patch management solutions that far exceed the capabilities of traditional manual processes.

Traditional software patch management often relies heavily on labor-intensive methods, which can become both time-consuming and inefficient. According to IBM research, it takes an average of 277 days to detect a breach, exposing organizations to prolonged vulnerabilities. The limitations of manual patch management manifest in three main areas: the necessity for IT teams to manually identify systems needing updates, the assessment of each patch's importance, and the sequential deployment of patches across the network. This slow and error-prone method proves inadequate against the backdrop of rising cyber crime rates and increasingly sophisticated attacks.

One of the significant drawbacks of manual patching is its reactive posture, wherein patches are typically applied only after known vulnerabilities are exploited. This delay can provide cyber criminals with critical time to attack systems. Moreover, flaws in patch releases can sometimes occur due to human error, a factor that automated systems, particularly those leveraging artificial intelligence (AI), are designed to circumvent by identifying code anomalies more efficiently than humans.

Automated patch management employs software tools to autonomously detect, download, and apply updates across an organisation's IT environment. Its key features include:

**Continuous Vulnerability Scanning**: Automated systems seamlessly integrate with existing vulnerability scanning tools to consistently monitor for known vulnerabilities. Upon detection, these systems identify affected devices and prepare them for prompt patching—effectively eliminating delays associated with manual processes.

**Real-time Prioritisation**: Automation tools connect with threat intelligence feeds to intelligently assess the urgency of patches based on vulnerability severity, the affected system’s importance, and the potential impact on business operations. For example, a critical patch for a core application can be prioritised above other less crucial updates.

**Automated Testing and Roll-backs**: To mitigate the risks of introducing instability through new patches, automated systems incorporate testing in isolated environments prior to full deployment. Should complications arise, such as a patch causing issues after implementation, the system can automatically revert to its previous state, thereby minimising downtime and preventing potentially far-reaching consequences.

**Real-time Monitoring and Alerts**: Enhanced monitoring features allow for continuous oversight of the patching process. In cases where a patch deployment fails or post-implementation issues are detected, automated systems provide immediate alerts to IT staff. This proactive surveillance aids in identifying problems before they escalate into significant vulnerabilities.

By adopting automated patch management, organisations can significantly improve their security postures, reducing the time their systems are exposed to potential cyber threats. As businesses continue to navigate the complexities of modern infrastructures and cyber crime, these systems represent a crucial component of an effective IT security strategy, freeing up valuable resources and ensuring compliance amid rapidly evolving threats.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.getastra.com/blog/security-audit/cyber-security-statistics/> - Corroborates the increasing frequency and sophistication of cyber attacks, including the average time to detect a breach and the rising costs of cybercrime.
* <https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/> - Supports the surge in cyber attacks worldwide, including the increase in attack frequencies and the sectors most targeted.
* <https://www.cobalt.io/blog/cybersecurity-statistics-2024> - Provides statistics on the projected costs of cybercrime, the rise in ransomware attacks, and the importance of proactive cybersecurity measures.
* <https://parachute.cloud/cyber-attack-statistics-data-and-trends/> - Details the frequency and types of cyber attacks, including malware and DDoS attacks, and the need for advanced cybersecurity measures.
* <https://www.nu.edu/blog/cybersecurity-statistics/> - Offers insights into the prevalence of malware attacks, the rise of malware-free attacks, and the importance of continuous vulnerability scanning.
* <https://www.getastra.com/blog/security-audit/cyber-security-statistics/> - Highlights the limitations of manual patch management, including the time taken to detect breaches and the reactive nature of traditional patching.
* <https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/> - Discusses the need for rapid and effective patch management solutions due to the increasing frequency of cyber attacks.
* <https://www.cobalt.io/blog/cybersecurity-statistics-2024> - Mentions the importance of real-time prioritization of patches based on vulnerability severity and business impact.
* <https://parachute.cloud/cyber-attack-statistics-data-and-trends/> - Supports the use of automated testing and roll-backs to mitigate risks associated with new patches.
* <https://www.nu.edu/blog/cybersecurity-statistics/> - Emphasizes the role of real-time monitoring and alerts in automated patch management to ensure continuous oversight and quick response to issues.
* <https://blog.checkpoint.com/research/a-closer-look-at-q3-2024-75-surge-in-cyber-attacks-worldwide/> - Highlights the benefits of automated patch management in improving security postures and reducing exposure to cyber threats.
* <https://news.google.com/rss/articles/CBMiqgFBVV95cUxNcEdLMExIcDN0M2FzR3JsRFI2WXZYVnFKWjRROE1JUFVnRU9zT0pNUTRqb2hFMWxicUZBNDh2NWxocHQ4Nk92b1hMQmo4Q1Jyc3ZTR1N0OGxVcmpkNVk0WHVEcTh3ZXJTV0tzRG5SS29EOVpMaV8zTUFnNXpjWS01WVVsVEN3MVBKLXJQbEJoemlQSlJ1Z0hoRW9uN1RBbDZJZlZFd3B6MmJTQQ?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data