

TABLE OF CONTENTS

The Objective	2
The Need For A Patching Cycle	2
Maintenance Windows	3
Workflow Automation	3
Endpoint Groups	4
Vulnerability Reports	5
Remediation Plan	6
Predictive Patching	7
Summary	8

THE OBJECTIVE

- When it comes to software patching, your company's goal is to reduce its security risk exposure as much as possible and as fast as possible. This can be done by ensuring that its computing environment and IT software stack are up-to-date regarding known vulnerability releases and patch upgrades. However, companies also need to meet objectives of supporting business applications without interruptions from endless maintenance and downtime cycles. Thus, there is an inherent tension between security and productivity, between managing risk and maintaining routine business operations.
- The JetPatch solution provides the means for Security, IT Operations and Compliance teams to balance these needs - reducing risk exposure duration as much as possible, while at the same time allowing computing and IT software to be fully utilized for their primary purpose – facilitating the goals and needs of the business. It empowers businesses to optimize computing resource usage while keeping company data and assets secure.
- JetPatch provides key stakeholders, such as CISOs and CIOs, with visibility into and governance of the end-to-end patching process, as well as detailed compliance reporting.



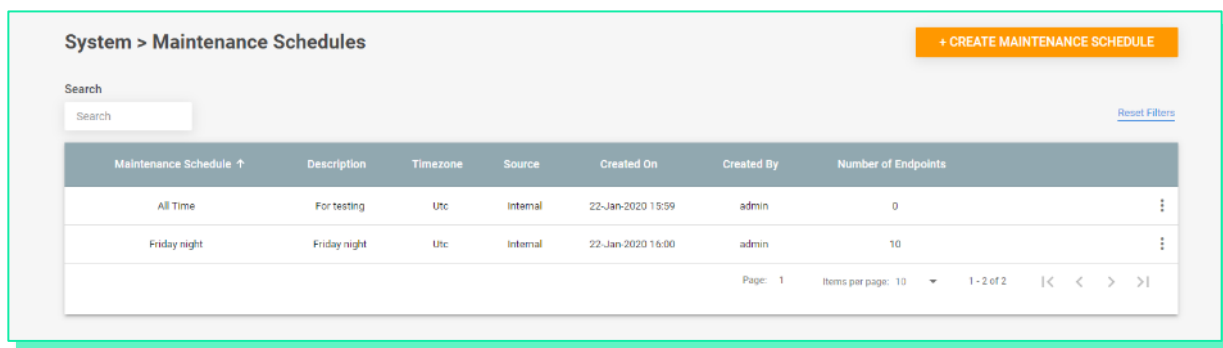
THE NEED FOR A PATCHING CYCLE

- Ultimate goal of IT and info security teams is clear: **Every endpoint** must be 100% compliant at **any given time**.
- Due to the dynamic nature of the security world, however, achieving this is almost impossible. In fact, even as patches are being executed to a group of endpoints, it is very likely that a newer version of one or more patches will have already been issued by the patch vendor. IT and security teams simply cannot invest all their time in 'chasing' endpoint vulnerabilities and successive patch releases.
- On the other hand, no IT environment can be patched once in a year and still be considered risk-free and compliant. With many organizations handling hybrid environments of both on-premise and cloud, the challenge of remediating all vulnerabilities across all environments at all times is insurmountable via existing processes.
- A Patching Cycle is a routine process through which companies execute an installation program that consists of a set of patches to be installed on a set of target endpoints. A good balance between endpoint compliance and both IT effort and work interruption can be achieved by patching each endpoint nearly **once every month**. This 30-day window is also considered as a best practice by the various compliance frameworks (e.g., HIPAA).
- From time to time, though, an urgent need to patch the environment arises as a result of new high-security risks and new vulnerabilities, such as zero-day threats. Every patching solution should be able to create an **emergency patch** and deploy it outside of the regular patching cycle.

MAINTENANCE WINDOWS

- The concept of a maintenance window plays an important role for every IT organization. Endpoints are actually patched only within this window during the patching cycle, generally at night and usually over the weekend.
- Maintenance windows allow relevant stakeholders such as IT operations, security teams and application owners to ensure that all is ready for the patching operation, yet impact on business operations and end users is minimal. With many organizations operating on a global scale across multiple time zones, finding that right 'golden' moment to patch an endpoint is a real challenge. Therefore, the ability to optimize patching success and maximize throughput is critical.

JetPatch Recommendation: To enable endpoint patching in a scaled environment, we recommend no more than **10 maintenance windows per patching cycle**, subject, of course to consideration of the CISO, IT-manager and application / services owners based on their assessment of business needs.



Maintenance Schedule ↑	Description	Timezone	Source	Created On	Created By	Number of Endpoints
All Time	For testing	Utc	Internal	22-Jan-2020 15:59	admin	0
Friday night	Friday night	Utc	Internal	22-Jan-2020 16:00	admin	10

WORKFLOW AUTOMATION

- Due to the complexity of today's IT infrastructure, when patching an endpoint, multiple operations must often be run prior to and after the actual patching. Nowadays, no endpoint resides in isolation, but is rather as part of a cluster, whether on-premise or on private or public clouds. Each is controlled by a specific group and adheres to different regulations and 'modus operandi'.
- Common endpoint pre-patch preparations include checking disk space, shutting down critical applications, creating a backup image of the endpoint (in preparation for a worst-case scenario), separating the endpoint from its current cluster and more. Post-patching activities may include clearing unrequired files, starting applications, executing a reboot -- or multiple reboots -- and validating of system status prior to going live.
- Orchestrating this sequence of actions is not an easy task, since it generally involves multiple people and combinations of manual and semi-automatic processes.

- JetPatch provides a dynamic and easy-to-use workflow mechanism that orchestrates all tasks. Once plugged into the workflow automation, no manual intervention is required. The JetPatch workflow interface can be customized to support the specific pre- and post patching-related tasks of each organization and create an automatic chain of events.

System > Workflows

Search

Search

Reset Filters

Workflow Name ↑

Description

Operating System

Created On

Status

Created By

Linux Critical Applications	SAP tests and reboot	Linux	22-Jan-2020 16:03	● Idle	admin	⋮
Patch Linux	Automatically created by the system	Linux (Default)	21-Jan-2020 11:40	● Idle	Policy Manager	⋮
Patch Solaris	Automatically created by the system	Solaris (Default)	21-Jan-2020 11:40	● Idle	Policy Manager	⋮
Patch Windows	Automatically created by the system	Windows (Default)	21-Jan-2020 11:40	● Idle	Policy Manager	⋮

Page: 1

Items per page: 10

1 - 4 of 4

< > >>

ENDPOINT GROUPS

- One of the primary steps in creating an enterprise patching strategy is to split endpoints in the environment into several reference groups, according to severity levels. The main purpose is to help the operations team to prioritize patching cycles, which are already complex. Categorizing endpoint groups according to asset importance allows for more effective decision making, as well as enabling quick reaction in the event of an emergency cycle, such as when a zero-day patch is required.

Four elements should be taken into account when defining endpoint groups:

- Importance - Each organization should know which are the most critical applications and services running on the computing environment. Those assets can be ERP systems, databases, email servers, web servers and so on. To assess the importance of each endpoint to the organization, the IT team should ask several questions:

- Are the applications running on the endpoint critical for the organization?
- Is the endpoint in the production environment? Or is it used for testing?
- If the endpoint is vulnerable, what will the impact of a breach be on my organization?
- Operating system - Different people in IT/security manage different types of endpoints. Usually, in an enterprise organization there will be separate IT/security teams for Linux and Windows, each responsible for applying patches and managing the assets for which they are in charge.
- Application owners - In some cases, application owners are also responsible for the resources running their applications, which adds another layer of complexity.
- Patching designation - Every software patch has its own category, such as security vulnerability, bug-fix, driver update, stability issue, and others, which may be applied to a different set of endpoints.

- To make the patching process manageable, it is recommended to execute patching workflows at the group level. In the event that different patching workflows will be executed on different endpoints, we recommend separating those endpoints into different groups.
- JetPatch Recommendation:** We recommend having 3 main types of endpoint groups:
 - Production endpoints with critical applications such as database instances or ERP related servers.
 - Production endpoints with non-critical applications for internal use, like Sharepoint endpoints.
 - Non-production endpoints for testing and/or other development purposes.

	Production with critical applications	Production with non-critical applications	Non-production
Security patches	All security patches are recommended	Only critical and important	Only critical
Other types of patches	All patches are recommended	Based on CISO - IT manager decision	Not needed

The above should be regarded as a general recommendation. However, a more accurate analysis of needs should be done by the CISO, CIO and other relevant stakeholders.

VULNERABILITY REPORTS

- Visibility into the overall patching process via vulnerability reports created and generated by vulnerability scanning systems is key for guaranteeing security risk reduction and governance. These systems constantly scan the environment for threats and issue alerts based on a real-time database of known security threats. This helps organizations be proactive in remediating vulnerabilities. These tools, when used regularly, contribute to the overall enterprise security posture and add an additional layer of validation and information to the compliance environment.

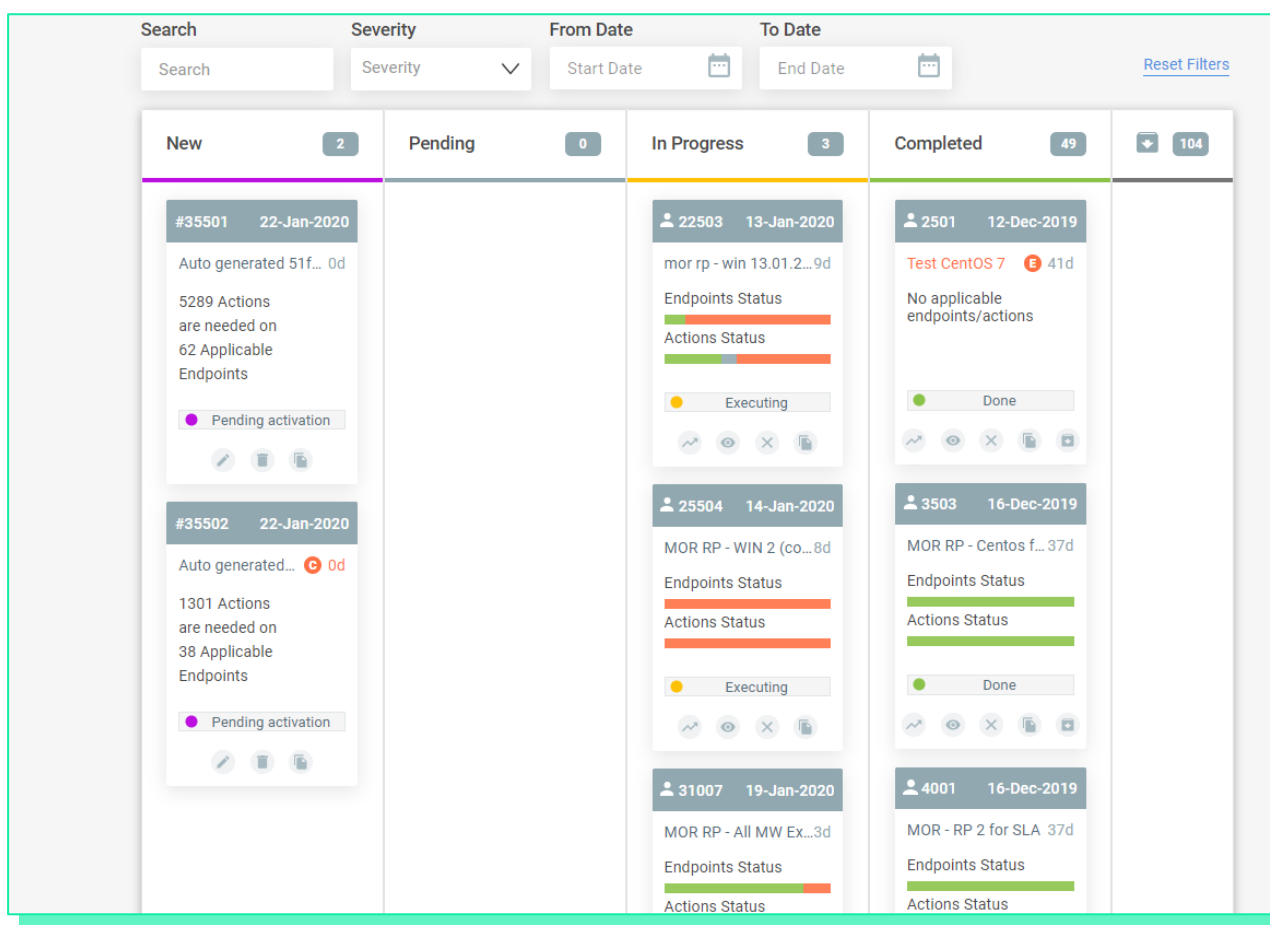


Patch Title	Operating System	Product	Category	Severity	CVE	Release Date	Remediation Plan	Needed On	Vulnerability
☐ RHSA-2018:1200 Important: patch security update	Red Hat Enterprise Linux 7.x x64, Unknown	Red Hat Enterprise Linux 7	Security	Important	Cve-TfAKE...		35501	1	Not Approved
☐ SUSE-SU-18:0152-1 Security update for samba	SUSE Linux Enterprise Server 12 x64	SUSE Linux Enterprise Server 12 (x86_64) SP 5	Security	Moderate		21-Jan-2020	35501	1	Not Approved
☐ SUSE-SU-10:0146-1 Security update for Mesa	SUSE Linux Enterprise Server 12 x64	SUSE Linux Enterprise Server 12 (x86_64) SP 5	Security	Moderate		21-Jan-2020	35501	1	Not Approved
☐ SUSE-SU-10:0145-1 Security update for Mesa	SUSE Linux Enterprise Server 12 x64	SUSE Linux Enterprise Server 12 (x86_64) SP 4	Security	Moderate		21-Jan-2020	35501	2	Not Approved
☐ SUSE-RU-18:0144-1 Recommended update for yast24csc-client	SUSE Linux Enterprise Server 12 x64	SUSE Linux Enterprise Server 12 (x86_64) SP 4, SUSE Linux Enterprise Server 12 (x86_64) SP 5	Recommended	Moderate		20-Jan-2020	35501	2	Not Approved
☐ SUSE-RU-12:0141-1 Recommended update for	SUSE Linux Enterprise	SUSE Linux Enterprise							

- JetPatch provides straightforward integration with various vulnerability scanning tools, including customization based on changing needs. This capability allows vulnerability data to be imported into the system with recommended patch remediation, which can be implemented using JetPatch's strong Remediation Plan engine.

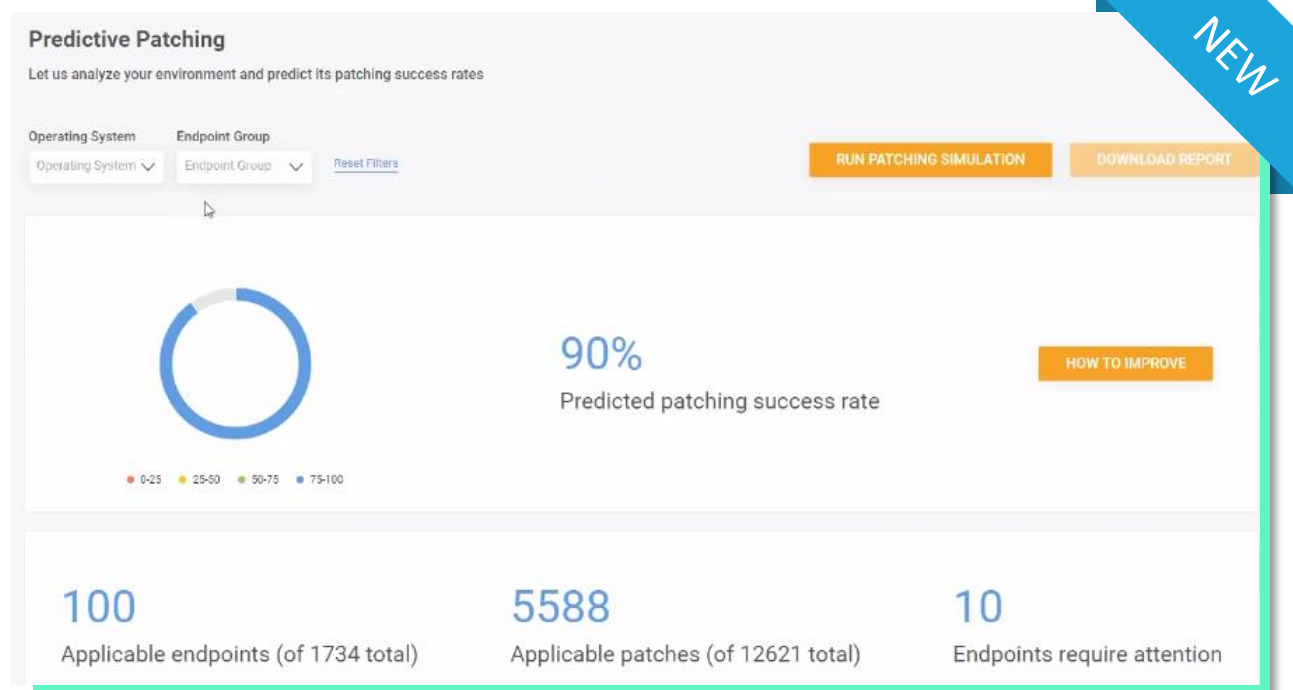
REMEDIATION PLAN

- Once the endpoints for remediation have been identified, endpoint groups have been assigned, relevant patches have been assembled from multiple resources, and process steps have been planned, it is time for the real action - execution.
- In contrast to common patching cycles, JetPatch's Remediation Plan encapsulates all these capabilities and requirements in a single consolidated view that allows stakeholders to follow the entire process in real-time via a modern Kanban-like board view. This main control offers full visibility and optimizes the patching process, simplifying complex, multi-step operations and manipulations.



PREDICTIVE PATCHING

- There are many reasons why patches fail during the patching process. Some common reasons include endpoints that are turned off, invalid credentials, expired licenses, low disk space, and unknown dependencies.
- Until now, the vast majority of these blocking issues were only discovered by teams after they attempted to implement the patching cycle. As patching cycles might take several hours to run, and are performed within a strict downtime window, failing to achieve a high patching success rate results in one of two outcomes:
 - Vulnerabilities are not remediated until the next maintenance window (by which time more things may have changed or broken), leaving endpoints vulnerable.
 - Another downtime window must be scheduled, potentially hurting the business.
- JetPatch's Predictive Patching allows IT teams to simulate the patch process before deploying the actual patch cycle. Using industry best practices, machine learning and correlation algorithms, the simulation exposes any potential problems that might occur during the patching cycle. The result is a detailed forecast of the expected success rate as well as analysis of the issues that should be addressed to improve it. Teams can now run patching cycles with much greater confidence and ensure maximum patching success.



SUMMARY

- The threat landscape continues to evolve, with sophisticated vulnerabilities introduced on a daily basis. Increasing IT and security staffing to actively remediate vulnerabilities is not a viable solution and cannot solve the problem. The fundamentals of cyber hygiene call for an innovative approach that can effectively handle the constant flow of software updates and the full range of computing environments, operation systems, endpoints and applications.
- JetPatch's ecosystem approach leverages existing security and IT systems in order to automate the overall vulnerability remediation process within existing organizational policies. By harnessing an intelligent workflow engine and adding machine learning capabilities to predict and optimize patching cycles, JetPatch provides IT and security leaders with governance of the overall remediation process, coupled with cost-saving and operational efficiency.



JetPatch

Next Generation Vulnerability Remediation!

About JetPatch

JetPatch cloud-based solution disrupts the domain of Vulnerability and Risk Management by introducing an ecosystem approach to vulnerability remediation and patch management. JetPatch orchestrates end-to-end remediation, using intelligent workflow automation - powered by machine learning capabilities. With JetPatch, enterprises proactively reduce security risks and achieve continuous compliance, while gaining operational savings across their complex IT environments. © 2020 JetPatch. All Rights Reserved.