secpod

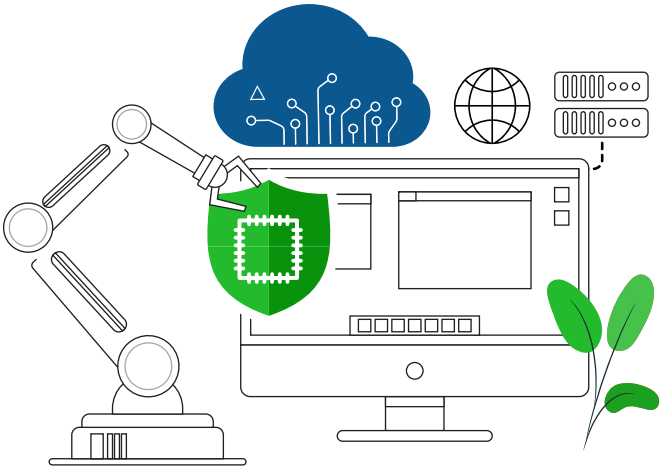
6 USE CASES OF SANERNOW'S AUTOMATED PATCH MANAGEMENT

www.secpod.com

Patching endpoints is the most basic prevention measure to mitigate vulnerabilities and keep away resource-draining security breaches. According to a **study**, more than 81% of businesses suffered an attack in the last two years. The technical causes were phishing attacks (36%), missing OS patches (30%), missing application patches (28%), and OS misconfigurations (27%). Hence, by streamlining and tightening the patching process alone, you can prevent more than 85% of attacks.

In most organizations, patching tasks are executed manually or using multiple tools that supporting different OS platforms. While it is appreciated that companies are making an effort to keep their systems updated, the real focus should be on actually reducing the risk scores with timely patching. **On average, organizations take 12 or more days to deploy a patch, which is more than enough time for a threat actor to unleash an attack.**

In a **study** named "Costs and Consequences of Gaps in Vulnerability Response", IT admins were asked which steps would improve their patching the most. Automation was voted (45%) as the most impactful security measure to improve patching.



Round the clock patching with SanerNow automated patch management

SanerNow Patch Management automates the end-to-end tasks of patching from scanning to deployment for effective reduction of the attack surface, a compliant environment, and an enhanced security posture. It also supports patching for all major OSs such as Windows, Mac, and Linux, missing configurations, firmware, and 200+ major third-party applications. As it operates on the cloud, it effectively manages remote devices without any perimeter limits to thwart cyberattacks across boundaries.

Six scenarios where SanerNow's automated patch management takes your patching miles ahead

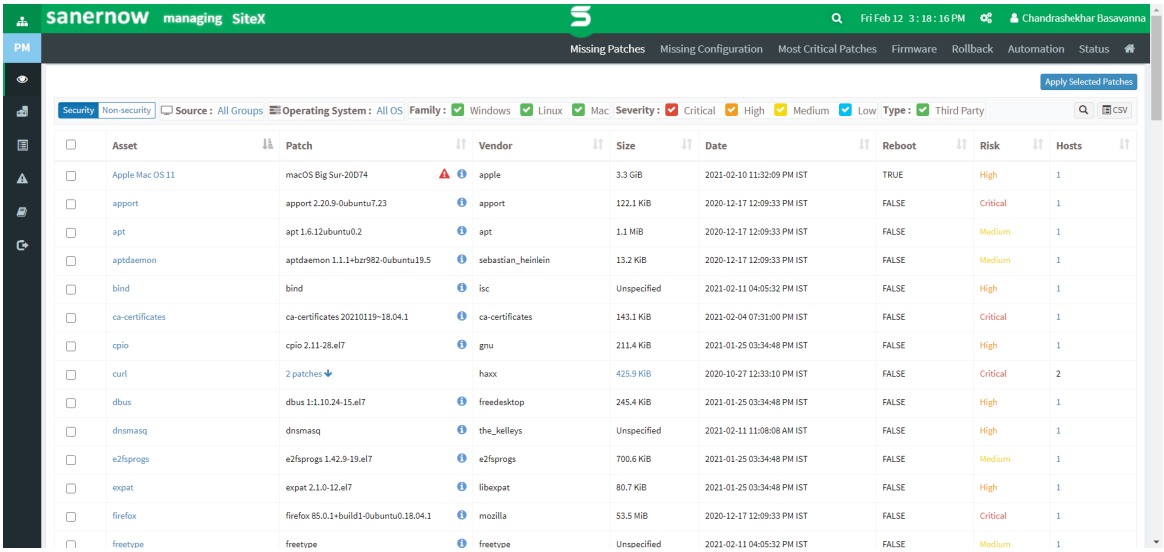
The below use cases are the highest level benefits that accelerate the patching process with automation and help reduce your attack surface quickly in the most efficient way.

01

Periodic patch scans failing to give real-time risk detection

Missing patches play a big part in the security and compliance posture of an organization. Organizations still rely on periodic scheduled scans to identify missing patches. Periodic patch scans are not sufficient to give real-time security exposure for companies. Running manual patch scans every few days do not guarantee active detection and elimination of risks. Moreover, the security team **cannot actively look for new patches** from software vendors in their application portfolio every day. To keep security teams updated, you need capabilities to notify you about missing patches automatically.

SanerNow detects missing patches through its **scheduled** or **continuous scans**. You can set up the scanner to run according to your preferences. You can schedule scans to run at a particular time every day. The patch download time and CPU threshold can also be scheduled. After each scan, SanerNow displays all details of missing patches, devices, risk levels, etc., to give you an exact picture of what's happening in your patch management space.

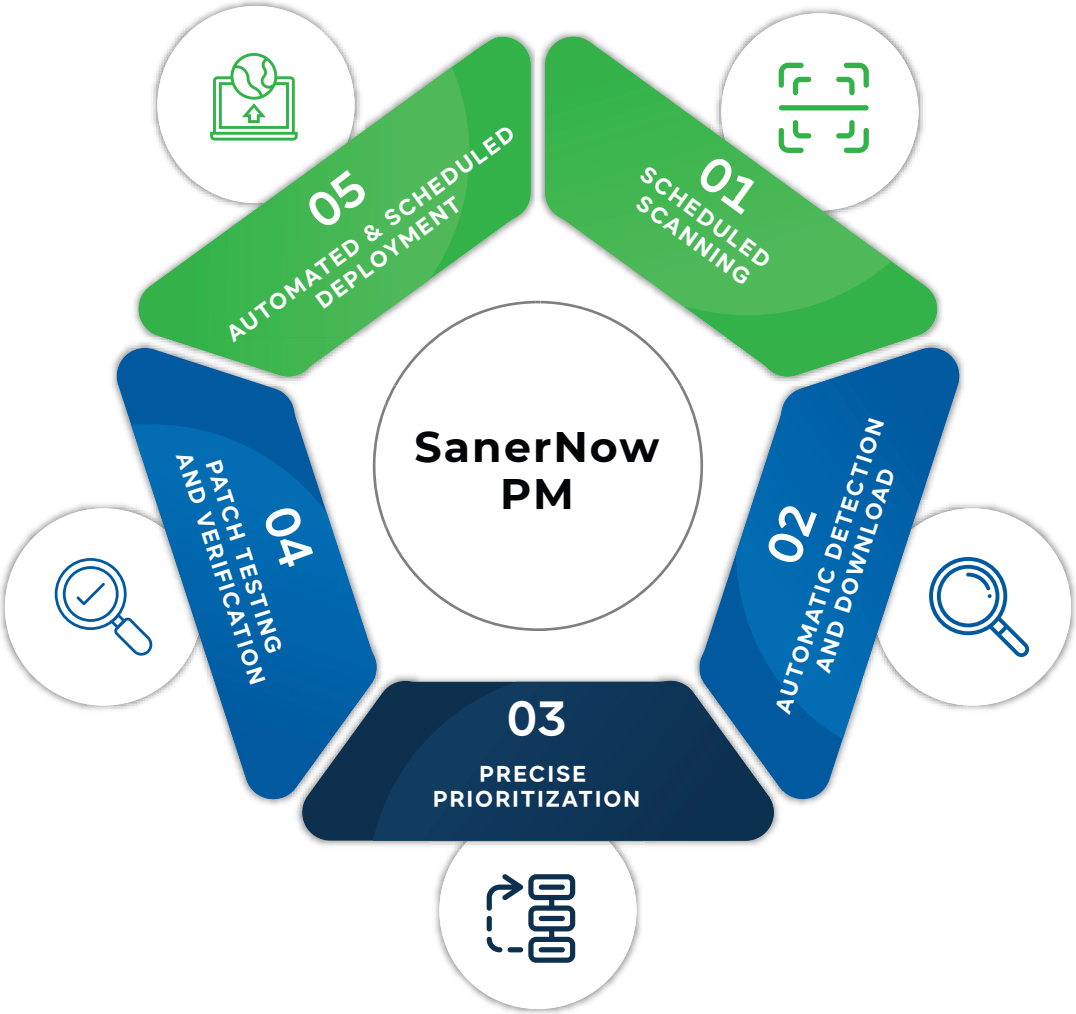


02 Manual patching tasks keeping teams on the run

Most companies (61%) feel that there are disadvantages for relying on manual processes for applying software patches.

The patching process is made up of many dynamic parts that require oversight. Manual patching tasks consume excessive time and demand a lot of resources. It involves patch scanning, detection, prioritization, download, testing, and finally, deployment. When multiple devices and IT technicians are involved, the process gets complicated.

Each time a patch job is needed, SanerNow executes a set of **standardized steps** in an automated way to ensure the fastest and most precise patching process. It performs automated scans, detection, and correlation of patches in vendor sites, accurate patch prioritization based on risk, one-time download and distribution, in-built testing, and scheduled deployment.

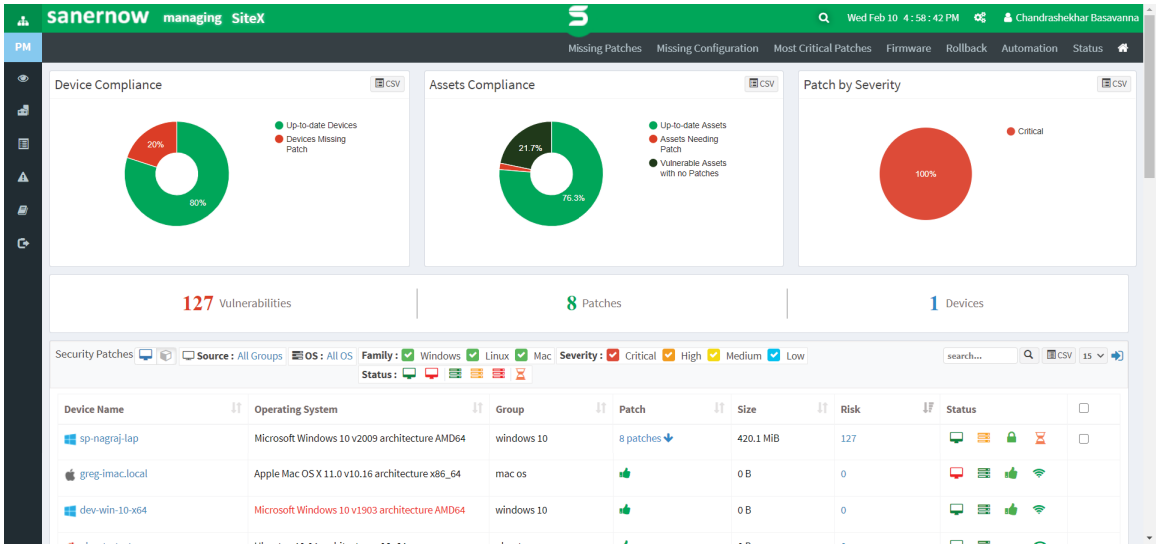


03 Compliance chores branching out additional tasks

Abiding with compliance benchmarks for patching is hectic and complex, especially during audits. Teams struggle to patch systems in time and show the compliance status of all endpoints collectively in their environment. They are either forced to switch between multiple tools or stuck with an ineffective tool that falls short.

To check if your environment is patch compliant in accordance with security benchmarks (ISO, NIST, PCI, HIPAA, etc.), SanerNow offers a readily built-in **patch compliance feature**. All non-compliant devices and their accurate severity levels are displayed. You can deploy missing patches and make sure all your devices are patch compliant. Get an exact picture of the security risks in the same view.

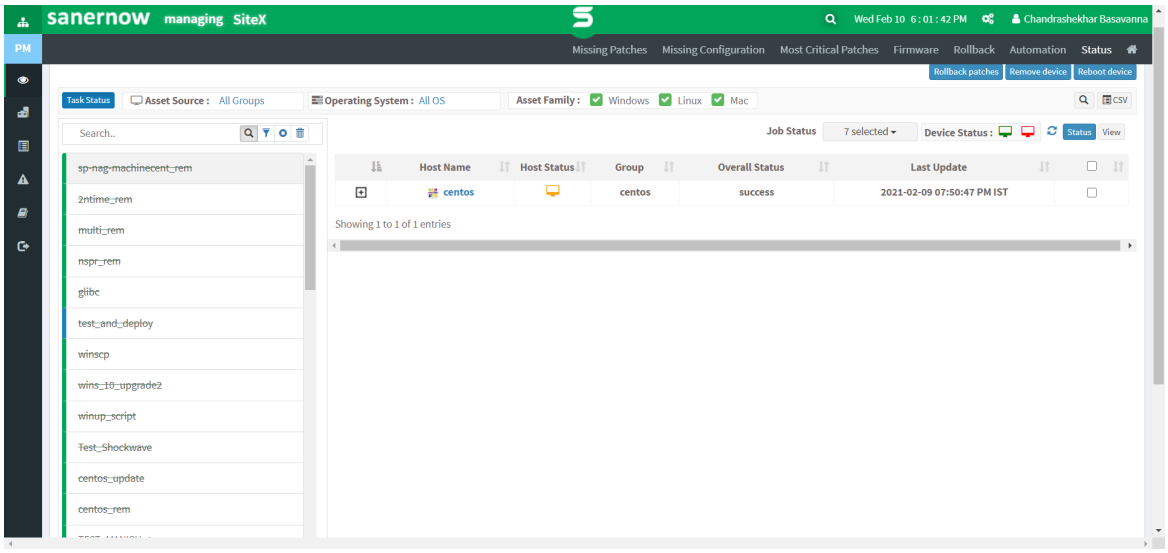
Additionally, when changes are made to security standards by the respective governing bodies, the **new policies are automatically updated** in SanerNow. You don't have to step in and update the policies manually.



04 One team, multiple patch jobs

Since patching is not a one-person and one-time task, they need to be executed and tracked continuously as a process. Most IT environments run multiple versions of different operating systems. When patch updates are released around the same time by different vendors, organizations may struggle to manually download each patch, deploy the right patch on the right device, and troubleshoot any issue that might stem from it. This is very exhausting in the long run.

SanerNow **accelerates each stage of the patching process** with automation and additional features to quicken the process with minimal supervision. You can create specific **patch jobs** for groups of devices and software and track them to finish. You can automate patching for specific operating systems **(Windows, Mac, Linux), missing configuration patches, third-party applications**, and **firmware**. Create jobs according to OSs, single/groups of applications, and department (device groups and Active Directory hierarchy). It has the capability to automate the entire patching cycle according to preset rules and conditions.



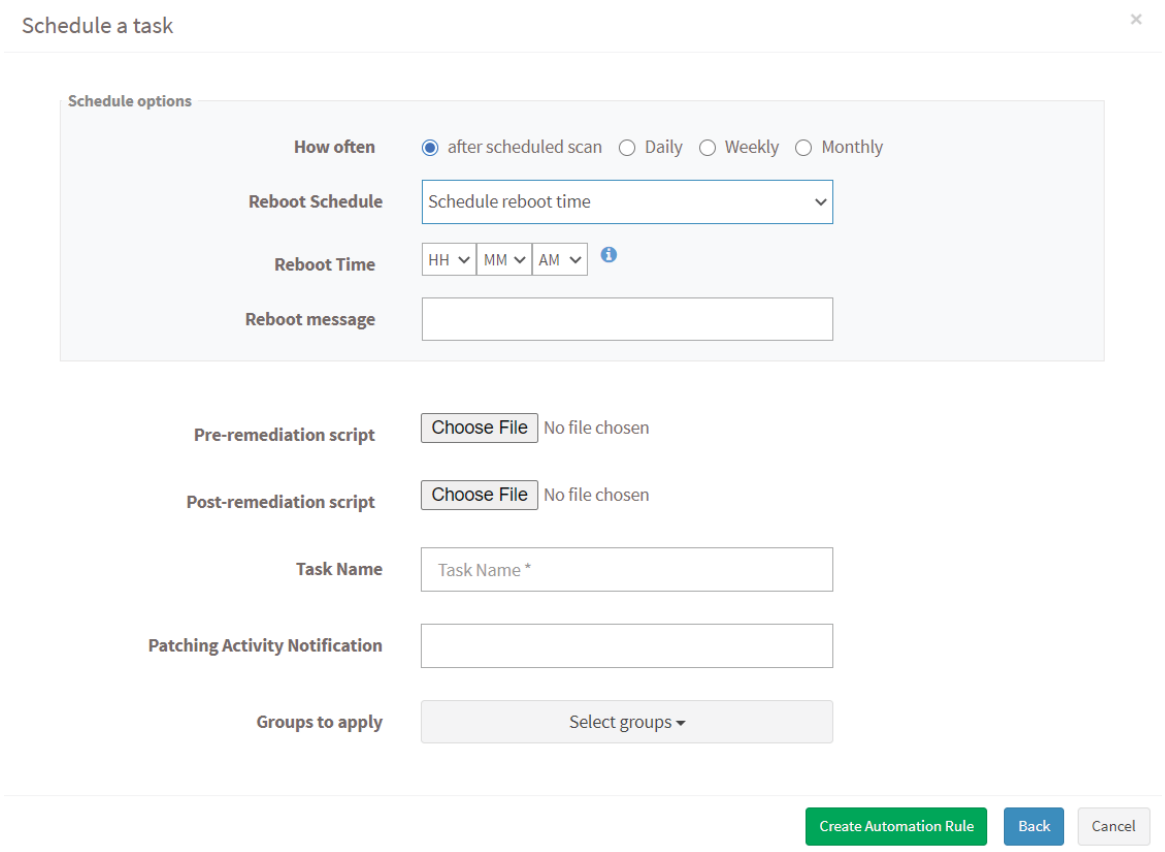
05

Missing auxiliary functions to complete patching

Most patching tools carry out the bigger functions but miss out on the small ones that are really important to complete and sign-off a patch job. When such small functions are missing, the security admin needs to step in and perform manual tasks, which again introduces delays and errors.

SanerNow offers a **reboot schedule** function integrated with its patch automation rules. You can schedule monthly, weekly, daily, or scheduled reboots according to your requirements to run the latest version without delays.

SanerNow supports new patches offered by vendors **within 24 hours of release** to ensure quick risk mitigation. **All patches are pre-tested** to check for any compatibility issues and errors. When an important update is released by a vendor, SecPod also sends out email alerts to make sure you don't miss them. After the patches are deployed, SanerNow performs a **final patch verification** on the device to check the patch status. SanerNow also packs additional handy features such as **patch rollback** to provide additional control over patch jobs.

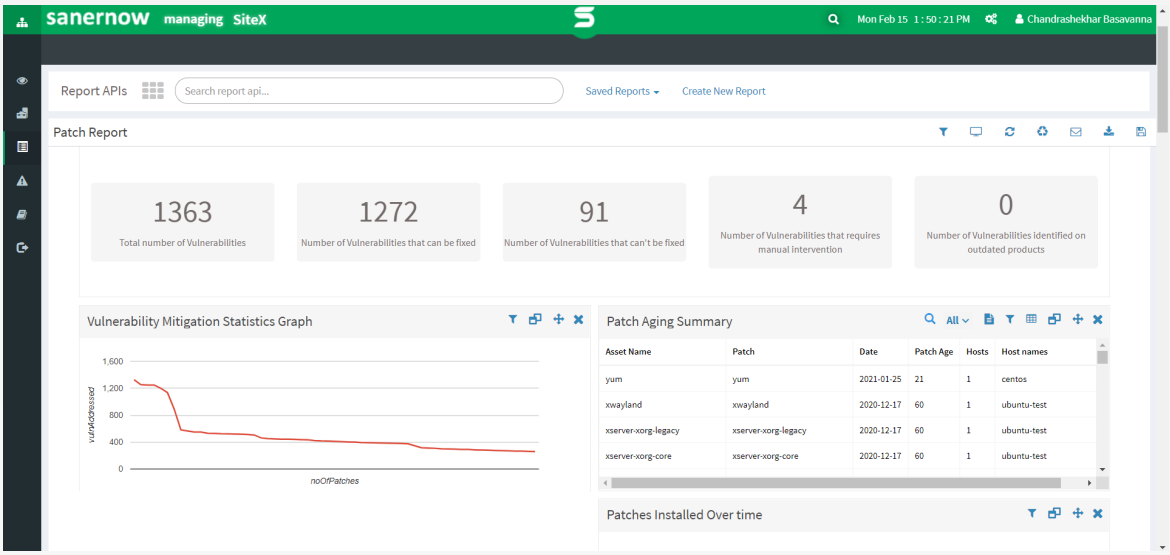


06

Difficulty in generating reports for audits and analysis

The close correlation of patching with business risks has made patch reports an important metric in the eyes of top management. When a higher official demands to read and analyze the security risks of an organization, patch reports are at the top of the list. You shouldn't struggle to put together the numbers into easily readable reports with the help of the same tool.

SanerNow offers **auto-generated, audit-ready reports** ready to be exported as **CSVs/PDFs** or emailed directly to a designated recipient with an option to automatically email reports at specific intervals. The **reporting APIs** come in handy to create and save custom reports according to your specific requirements.



Rather than looking at patching as a routine day-to-day management task, it is pivotal to understand the massive positive impact it can create in reducing security risks. To deal with the growing number of cyber-attacks and security breaches, implement an automated mechanism to minimize the threat surface actively. Scale up your patching game with automation capabilities and strengthen your security posture.

Patch like a pro with SanerNow Automated

Patch Management

Schedule a free demo