secpod

INTEGRATED VULNERABILITY & PATCH MANAGEMENT

Your First Step Towards Endpoint Security Brilliance

www.secpod.com

Why Integrated Vulnerability and Patch Management is the First Step Towards Endpoint Security Brilliance

2020 is a year where a new digital era began, bringing multiple changes to the world and how businesses operate. As the pandemic poses numerous challenges to different walks of life, IT security is no exception. Organizations have adopted the new "work from home" norm to battle COVID-19, and their endpoints are now distributed at different locations. This unprecedented transition has not only brought new changes to the IT infrastructure, but it has also opened up new gateways for attacks, having a stronger effect on the threat landscape.

To make the existing situation even more challenging, 2020 has seen a rapid increase in the number of vulnerabilities disclosed in the first half of the year, and this count is expected to exceed that of last year. A **study** shows that Microsoft has seen a 150% increase in the number of vulnerabilities disclosed during the first six months of 2020 compared to the entirety of 2019. Windows 10 was the product with the most disclosed vulnerabilities by the end of Q2.

The alarming stats and the new working norm have put IT Teams in a tough spot to rethink and re-align their current vulnerability management strategy to cope with the upcoming trend.

The common approach:
Vulnerability management through siloed interfaces

In the early 2000s, the number of vulnerabilities discovered in a year was in thousands, and IT teams managed them through manual scans, assessment, and remediation techniques. With the shift to modern environments, IT security administrators soon found the old approach ineffective. They started bringing in the latest tools to carry out each vulnerability management task: An effective scanner to detect the network's vulnerabilities, an advanced assessment tool to evaluate each vulnerability, and a patch management solution to remediate the detected vulnerability. However, these siloed interfaces still didn't reduce organizations' risk exposure and made vulnerability management a more hectic task.

Dealing with vulnerabilities through siloes made organizations employ different teams to manage each process, making the whole task complex, time-consuming, and ineffective. These teams still find it hard to collaborate, understand, and envision an efficient strategy to analyze various vulnerabilities, their exploit potential, prioritization level, and remediation action. All these challenges inevitably let many vulnerabilities prevail unpatched in the network, opening gateways for attackers to exploit them.

Delay in remediating vulnerabilities increases security gaps

According to **Edgescan Stats Report**, an organization's average time to close a discovered vulnerability (caused by unpatched software and apps) is 67 days. Attackers are well aware that organizations take months to deploy unpatched vulnerabilities and are using this security gap to exploit the network. A **study** by Ponemon Institute states that 60% of breaches in 2019 were due to unapplied patches, which were readily available but not deployed.

From these stats, we can infer that organizations lack an integrated vulnerability and patch management technology to help them remediate the detected vulnerability without any security gaps.

Integrated vulnerability and patch management approach, a must-have today

The integrated vulnerability and patch management technology combats traditional vulnerability management challenges and proves to be more effective in reducing the organization's attack surface. From a single pane of glass, you will be able to view and manage the end-to-end vulnerability management process from scanning, assessment, prioritization to remediation without any delays.

Here are the reasons why an integrated vulnerability and patch management approach is the best fit for your security framework:

01 **Scale-up operational efficiencies:**

Orchestrate the end-to-end tasks of vulnerability management from a centralized console. Reduce costs on purchasing multiple point solutions, save time and resources spent on using swivel chair interfaces.

02 **Increased visibility:**

Gain 360-degree visibility over your organization's security exposure by combining all vulnerability and patch information in one view. This better visibility over your security posture will enable you to plan and implement effective operations.

03 **Smarter prioritization:**

By combining the discovered vulnerabilities and available patches, you can smartly prioritize them by assessing their risk and exploit potential in your network and plan necessary remediation measures.

04 **Faster remediation:**

With a unified view of both vulnerability and patch scan results, you can quickly identify which patches address the vulnerabilities and implement an on-demand work-flow to deploy these patches. This correlation will help you mitigate vulnerabilities quickly.

05 **Improved security and control:**

As you quickly remediate the discovered vulnerabilities in your net-work, you minimize the exploit potential to a greater extent and reduce your network's threat exposure.

SecPod SanerNow,

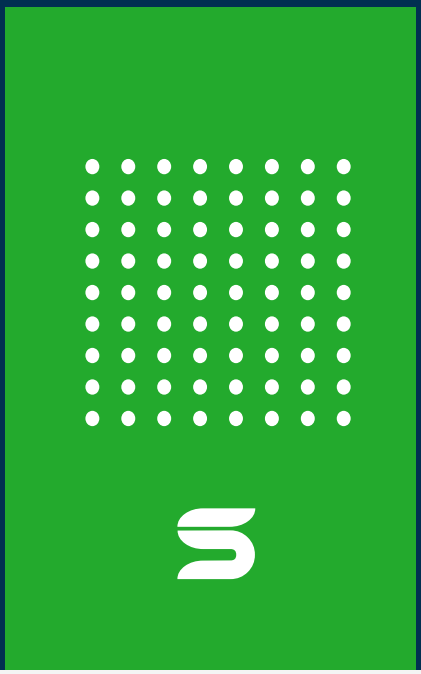
The integrated vulnerability & patch management solution

SecPod SanerNow is a cloud-based solution that integrates vulnerability and patch management solution in one centralized view. With SanerNow, you can remotely execute the end-to-end vulnerability management tasks from scanning, assessment, prioritization to remediation through one single console.

Leveraging the world's largest SCAP feed with over 100,000+ vulnerability checks, an intelligent algorithm to run the industry's fastest scans within 5 minutes, an integrated patch remediation technique, and end-to-end automation with an always-on continuous approach, SanerNow minimizes your organization's attack surface and strengthens your endpoint security posture.

With SanerNow, you can,

- **Manage vulnerabilities in heterogeneous OS endpoints**
- **Run rapid and continuous vulnerability scans**
- **Detect vulnerabilities accurately using a vast number of security checks**
- **Assess and prioritize high-risk vulnerabilities**
- **Remediate vulnerabilities with an integrated patch management technique**
- **Perform perimeter-less management on remote devices from the cloud**
- **Automate end-to-end vulnerability management tasks**



You can achieve all of the above with a "**one console and one agent approach**", minimizing your network resources and bandwidth consumption.

Your new IT infrastructure needs a more modern strategy to secure your endpoints.

Learn to unlearn the traditional methods, and it is time you implement an integrated approach to manage vulnerabilities.

Let SanerNow make it easy for you.

Schedule a Demo