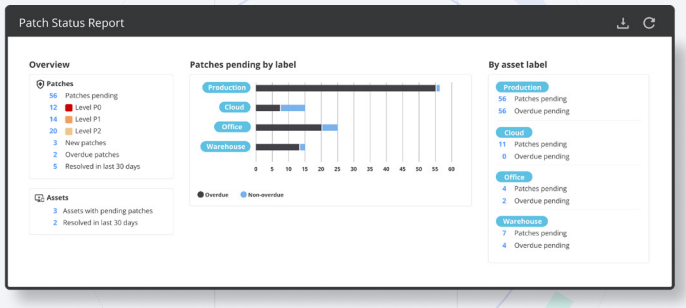
Nanitor

SECURITY COMPONENTS

Patch Management

Nanitor's patch management features help you keep track of pending security patches across your organization. Which assets are going unpatched, how many are overdue, how many patches have been installed in the last month - Nanitor gives a clear overview of the health of your organization's patch habits and helps you strengthen your security posture.



Key benefits

01

Prioritization in the Nanitor Diamond

Like other security issues, Nanitor will list missing patches on your assets as soon as they are detected, give them a priority rating, and show them in the Nanitor Diamond.

02

See assets that need patching

Easily view which assets are missing a particular patch in the patch detail view in a prioritized order, making it easy to identify the most critical assets that need patching.

03

Statistics on patch status

View statistics on patches in the patch status report - number of patches pending, new and overdue patches, how many at each priority level, and how many have been resolved (installed on all outstanding assets) in the past month.

04

Break down by asset label

The dynamic patch status report can be filtered or broken down by asset label, providing an easy overview of what kinds of assets in what departments need patching.

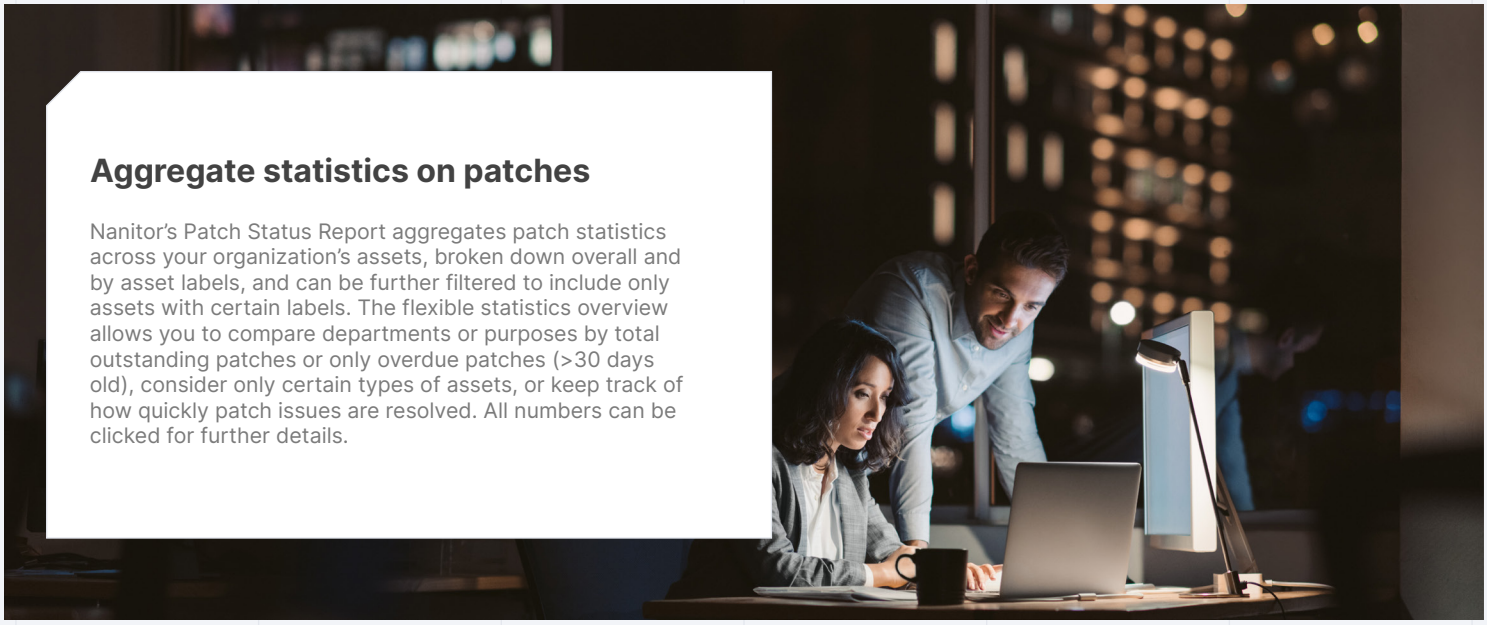
Unpatched systems are vulnerable to known exploits and often easily compromised.

Bugs and vulnerabilities are constantly being discovered and patched in the most widely used operating systems. If vital security patches are not installed within a reasonable timeframe, your organization is left open to hackers exploiting publicly known vulnerabilities.

Ensuring that security patches are installed in a timely manner across your organization's assets can be a difficult task, but it no less vital to the system's overall security posture.

Collecting your outstanding patches in one place

Nanitor's Discovery Engine quickly detects when a patch is missing on an asset and checks it in to your central Nanitor instance. Each patch raises an issue, which is prioritized alongside other security issues in your system based on the importance of the issue and assets where it is present. The issue detail page shows the vendor's information on the patch, what assets are missing this patch, and how critical those assets are, making it easy to tell which assets need patching first.



Aggregate statistics on patches

Nanitor's Patch Status Report aggregates patch statistics across your organization's assets, broken down overall and by asset labels, and can be further filtered to include only assets with certain labels. The flexible statistics overview allows you to compare departments or purposes by total outstanding patches or only overdue patches (>30 days old), consider only certain types of assets, or keep track of how quickly patch issues are resolved. All numbers can be clicked for further details.

What is Nanitor?

Nanitor is a powerful cybersecurity management platform focusing on hardening security fundamentals across your global IT infrastructure. The platform provides unique visibility and control of your security challenges that stakeholders can trust, at a fraction of the cost and time of alternatives.

Learn more at: www.nanitor.com
Email: sales@nanitor.com

The Nanitor Discovery Engine™

The Nanitor Discovery Engine™ gathers information about each of your organization's assets in real time - system information, user accounts, configurations, patch status, security vulnerabilities, installed software, and more. The data is collected on your company's central Nanitor server, where it can be viewed, searched and scrutinized by your security team, and any issues found can be consolidated and prioritized. All data stays internal - your company has its own Nanitor instance, safe from prying eyes.

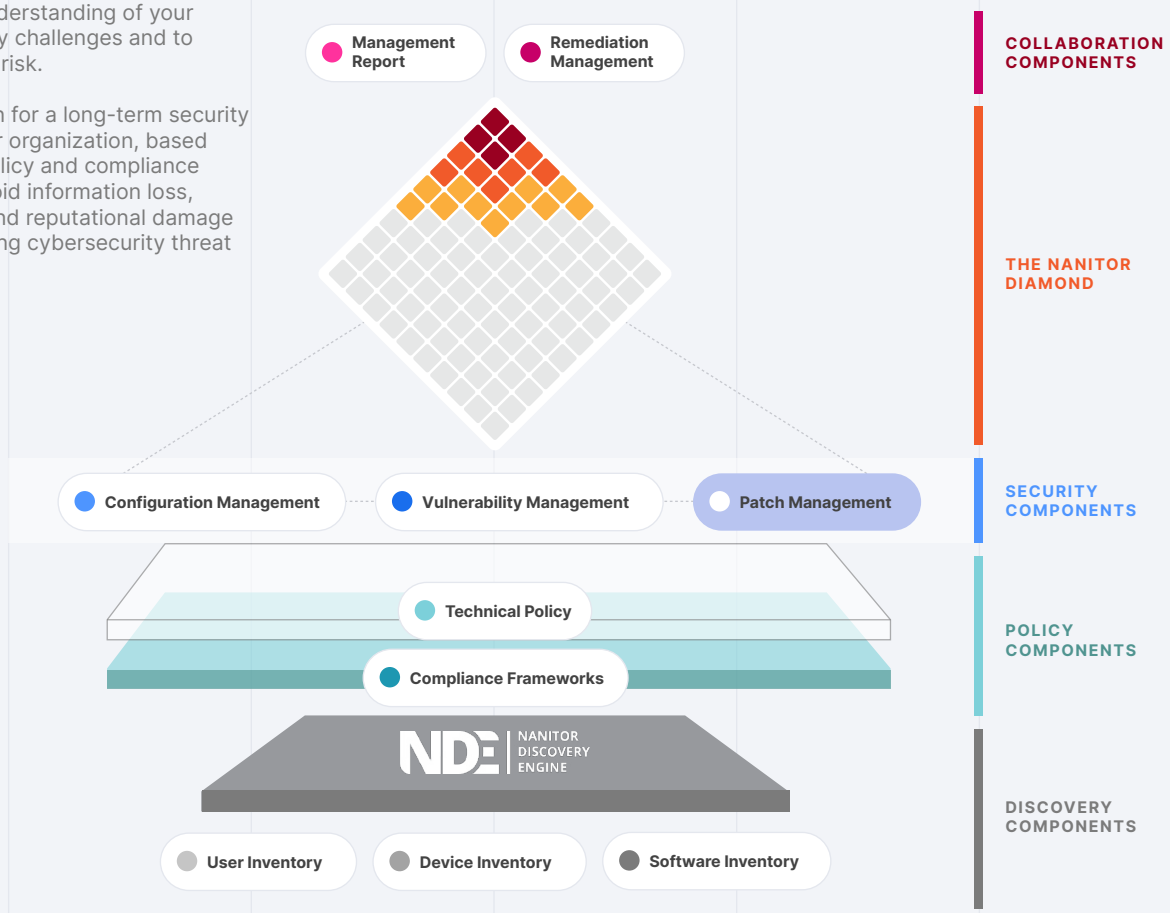
Employee workstations, servers and other assets can install the lightweight, cross-platform Nanitor Agent, an unobtrusive background process that monitors that asset and checks in to your Nanitor server with updates. Assets that cannot install software, such as network devices, can be monitored by the Nanitor Collector, a central service that regularly polls its assigned devices for information. By enabling the Network Discovery feature, Nanitor can automatically discover any rogue devices on the company network that are not yet monitored, helping you achieve full coverage.

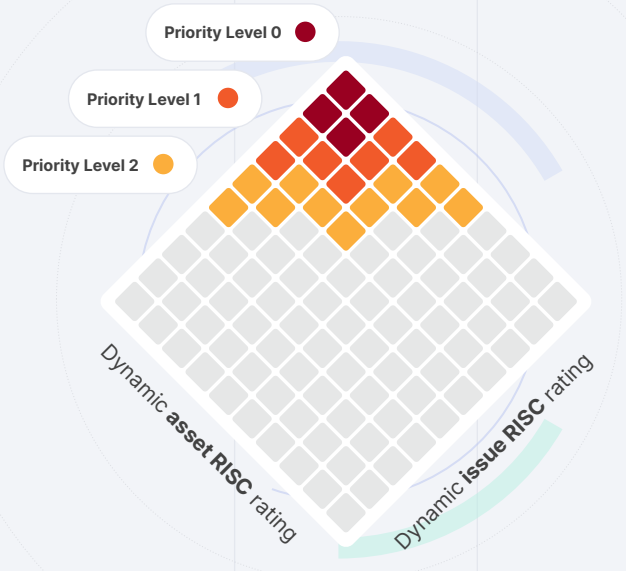
- **Lightweight**
- **Non-intrusive**
- **Self-regulating**
- **5-minute updates**
- **Running on more than 50.000 critical assets worldwide**

The Nanitor Platform

The Nanitor platform allows you to build a collective understanding of your fundamental security challenges and to quantify your cyber-risk.

It forms a foundation for a long-term security strategy across your organization, based on your technical policy and compliance requirements, to avoid information loss, service disruption and reputational damage from the ever-growing cybersecurity threat landscape.





The Nanitor Diamond™

The Nanitor Diamond™ shows an immediate visualized overview of all potential security issues found on your systems, broken down by issue criticality and asset criticality. With a glance at the top squares of the diamond, identify the presence of critical issues on your most important assets. Any square can be clicked for a further breakdown of the issues, what assets they exist on, and remediation instructions for each.

Nanitor prioritizes security issues by their potential impact on your organization - for instance, a critical unauthorized data access vulnerability will have a large impact if found on an important database server containing sensitive data. Issues are grouped automatically into priority groups by Nanitor's RISC score impact rating, providing a clear plan of action for your security team.

Rank the criticality of your assets based on customized system-wide labels that can be assigned manually or automatically, and Nanitor will intelligently adjust from there. Fine-tune Nanitor's default ranking of different kinds of issues to suit your organization's needs if necessary, and see your adjustments reflected in the diamond.