Nanitor

COLLABORATION COMPONENTS

Management Reports

Nanitor will generate a variety of printable PDF reports and portable CSV files convenient for data crunching. Data can easily be passed to collaborators, managers and auditors for a clean look at the security status of different parts of the system.

Key benefits

01

Readily available statistics

Nanitor's detailed reports generate notable statistics about your system on demand, allowing you to understand your security posture better and gain a fuller overview of the status of your assets.

02

Printable and portable

Nanitor's reports can be exported to PDF and printed, or simply sent to collaborators by e-mail to save paper, without having to give everyone who needs them access to the full Nanitor system.

03

More accurate reports in less time

Automated reporting saves time and improves accuracy. Generate security status reports you can trust with no fuss and no busywork, at the click of a button.

04

Flexibility

Nanitor offers a large variety of reports on different security topics. Depending on the report, options allow for including the entire organization or a subset of assets, choosing a time period to cover, or limiting the number of entries.

Diverse reports from the lowest levels to the highest

Nanitor offers automatic reports and exports of a variety of data at all levels of the system. They include:

- **Asset report:** List assets, their details, and any issues affecting them, for a given asset label or the entire organization - or export the asset list as a CSV file that can be processed by other applications.
- **Benchmark audit report:** For a given CIS benchmark, see how many assets are compliant with each rule, whether the rule is in your technical policy baseline, and any exceptions that apply and why.
- **Compliance report:** View the requirements of your assigned compliance framework along with issues associated with them and their priority category.
- **Trend metrics report:** Metrics and graphs showing changes over time in how many assets are monitored by Nanitor and how many issues affect them, with breakdowns on what has changed each month.
- **Patch status report:** Statistics on outstanding, overdue and resolved patches across the organization on a monthly basis.

Collaboration with others is part of any security workflow.

Whether it's a security audit, upper management or the system administrator tasked with resolving an issue, understanding the bigger picture and sharing information with others is a vital part of a healthy focus on security.

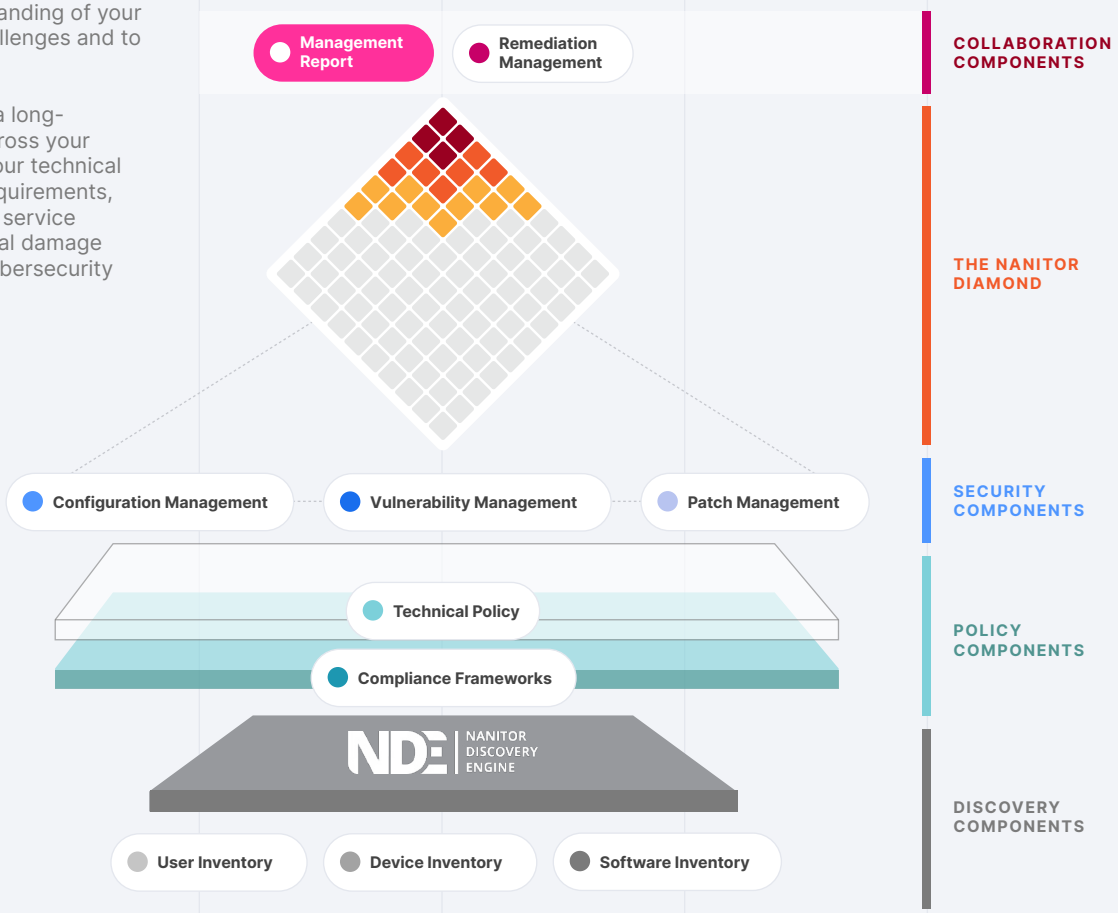
Robust reports on both the high-level statistics and the low-level details that can be shared with other parties facilitate good collaboration and communication about security.

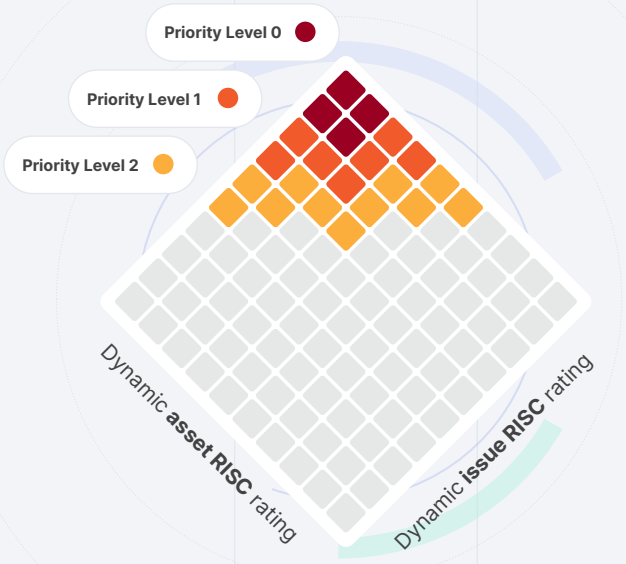
Learn more at: www.nanitor.com
Email: sales@nanitor.com

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.

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

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.

NDE™ Platforms

Nanitor's Discovery Engine supports collecting data from a large and growing number of platforms, spanning desktops, servers, network devices, applications and application servers, databases and cloud services, either by installing the Nanitor Agent or configuring the Nanitor Collector.

Cloud

docker, kubernetes, aws (Amazon Web Services), Google Cloud, Office 365

Network Devices

f5, Fortinet, JUNOS, hp, paloalto, UBIQUITI, Check Point, CISCO

Server

OpenBSD, ubuntu, SUSE, CentOS, Red Hat, aws (Amazon Linux), debian, Free BSD, AIX (IBM AIX), Windows Server

Desktop

mac OS, Linux, Windows

Application Server

Nginx, Microsoft IIS, Exchange

Application

Chrome, Internet Explorer, Microsoft Office

Database

MySQL, ORACLE DATABASE, PostgreSQL, Microsoft SQL Server