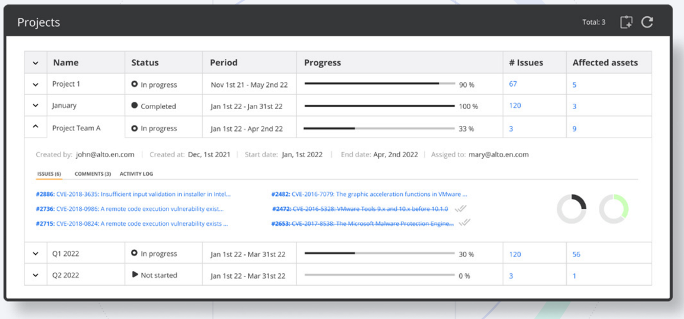
Nanitor

COLLABORATION COMPONENTS

Remediation Management

Nanitor's remediation management features help you organize your team to tackle the security issues flagged by the system. Organize your most important issues and affected assets into projects, assign a team member and a due date, and track incremental progress as your security is tightened.



Projects

Total: 3

	Name	Status	Period	Progress	# Issues	Affected assets
⌄	Project 1	○ In progress	Nov 1st 21 - May 2nd 22	90 %	67	5
⌄	January	● Completed	Jan 1st 22 - Jan 31st 22	100 %	120	3
^	Project Team A	○ In progress	Jan 1st 22 - Apr 2nd 22	33 %	3	9

Created by: john@alto.en.com | Created at: Dec, 1st 2021 | Start date: Jan, 1st 2022 | End date: Apr, 2nd 2022 | Assiged to: mary@alto.en.com

ISSUES (6) COMMENTS (3) ACTIVITY LOG

#2886: CVE-2018-3635: Insufficient input validation in installer in Intel...

#2736: CVE-2018-0986: A remote code execution vulnerability exist...

#2715: CVE-2018-0824: A remote code execution vulnerability exists ...

#2482: CVE-2016-7079: The graphic acceleration functions in VMware ...

~~**#2472:** CVE-2016-5328: VMware Tools 9.x and 10.x before 10.1.0~~ ✓✓

~~**#2653:** CVE-2017-8538: The Microsoft Malware Protection Engine...~~ ✓✓

	Name	Status	Period	Progress	# Issues	Affected assets
⌄	Q1 2022	○ In progress	Jan 1st 22 - Mar 31st 22	30 %	120	56
⌄	Q2 2022	▶ Not started	Jan 1st 22 - Mar 31st 22	0 %	3	1

Key benefits

01
Organize the remediation of issues

After security issues have been identified, Nanitor helps you break down remediation tasks into manageable projects, with each project either organization-wide or limited in scope to a particular set of assets, and provides the details required to resolve each issue.

02
Assign and schedule

Each project is assigned to a single team member who is responsible for that project. Projects can be given a due date or prepared in advance before work is started on them, keeping the team on track.

03
Track progress on security tightening

Projects have a 'progress bar' that advances with each time an issue is resolved on a given asset, providing an easy overview of how projects are progressing as you improve your security posture.

04
Automatic resolution detection

Nanitor automatically discovers when an issue has been resolved. No need to manually check off tasks and then bother QA to verify - when the issue is fixed, Nanitor picks it up and advances the project progress. Your team members can focus on just fixing the issues.

It's not enough to detect the security issues - you have to fix them.

Even when you have found security holes in your system, remediating those issues requires the manual intervention of people who understand the needs of the system and the security principles at stake. Problems often languish after detection when team members are overwhelmed and don't know where to start or who is responsible.

Security requires swift action and organization. Deciding who should act to fix issues and how and keeping track of how the work is progressing is necessary to achieve real results.

Monitor remediation progress

The Nanitor Project Inventory shows the status of a project, the current progress as a percentage of issues resolved on assets within scope, the due date, assignee, creator, and number of affected issues and assets. From there, drill down to see each project's assigned issues and their status on the individual assets within the project's scope. Keep firm track of what has been done, what is yet to be done and who is responsible for ongoing progress.

Flexible security remediation projects

When Nanitor has detected and prioritized security issues, you can assign a subset of them to a project. Assign a responsible team member, set a due date, and limit the scope to certain assets if necessary - have your server administrator handle the servers, or employees of certain departments handle that department's assets.

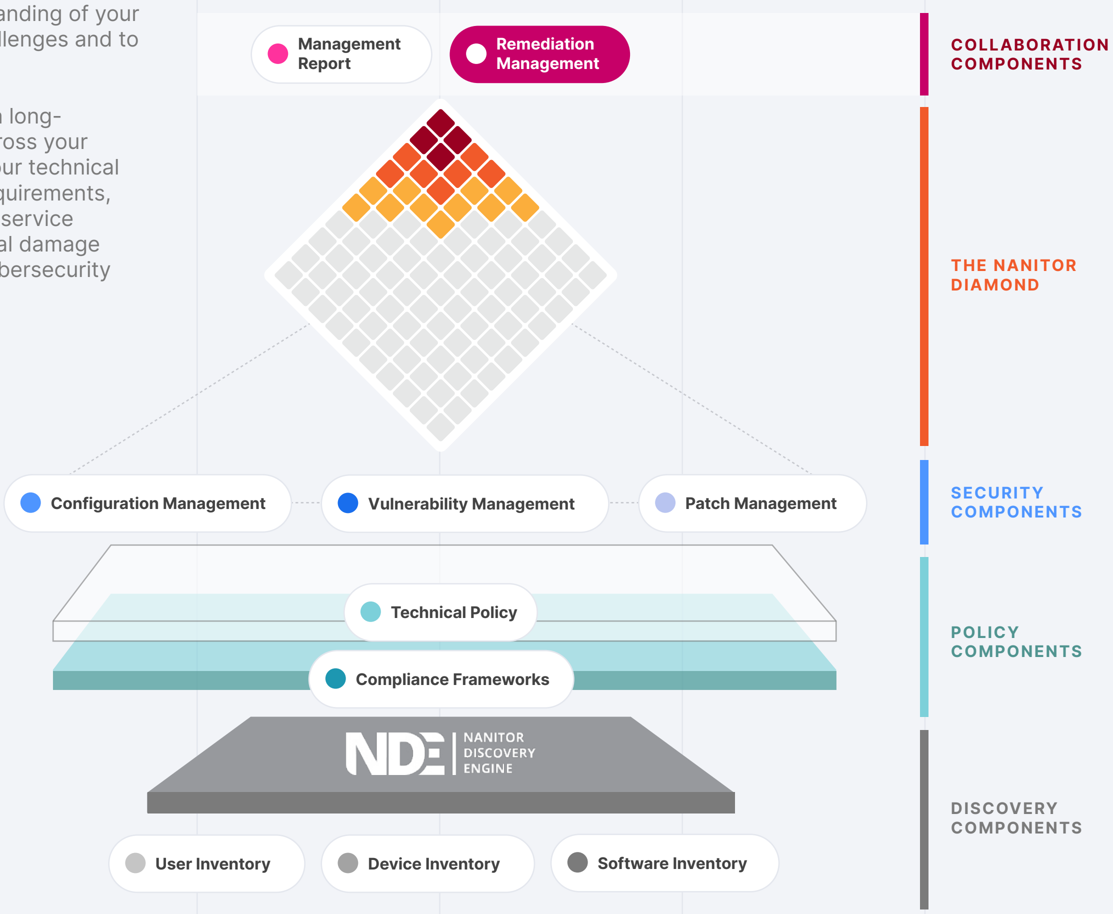
All your team members have to do is resolve the issues on the assets within the project's scope, and the project progress will update. If the security team determines that an issue is not a problem right now, exceptions can be added to treat the issue as resolved, either permanently or for a certain amount of time.

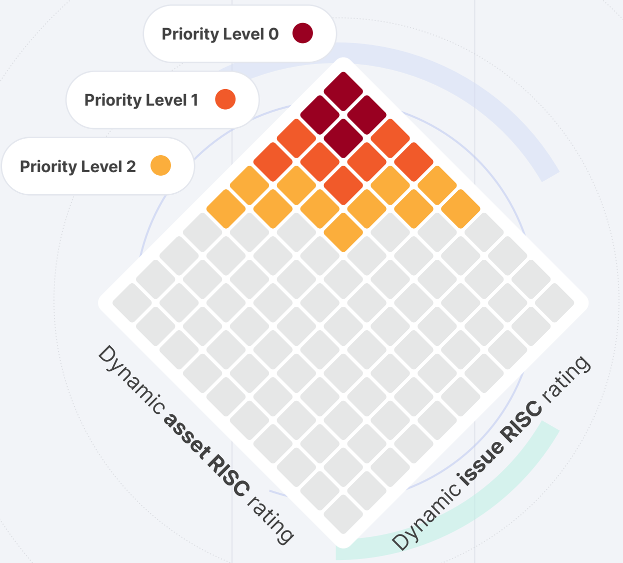
Learn more at: www.nanitor.com
Email: sales@nanitor.com

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.

NDE NANITOR DISCOVERY ENGINE
User Inventory
Device Inventory
Software Inventory

- ✓ 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

SQL Server