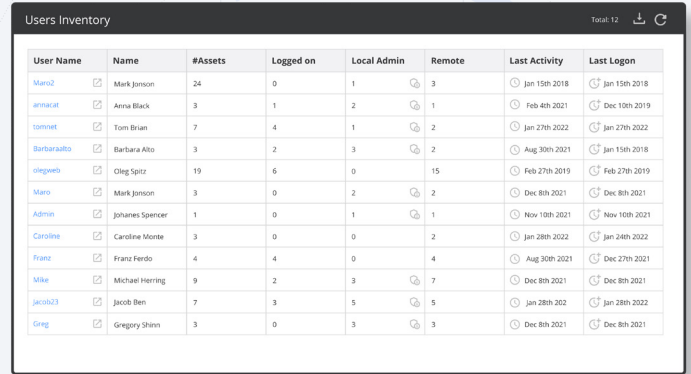


DISCOVERY COMPONENTS

User Inventory

The Nanitor User Inventory provides a sortable and filterable overview of all user accounts across your organization's assets. See who has an account on which devices, when they last logged in, whether they have admin or remote access, and whether they're flagged with issues such as expired passwords.



User Name	Name	#Assets	Logged on	Local Admin	Remote	Last Activity	Last Logon
Mark2	Mark Janson	24	0	1	3	Jan 15th 2018	Jan 15th 2018
anna1at	Anna Black	3	1	2	1	Feb 4th 2021	Dec 10th 2019
tom1net	Tom Brian	7	4	1	2	Jan 27th 2022	Jan 27th 2022
Barbaraalto	Barbara Alto	3	2	3	2	Aug 30th 2021	Jan 15th 2018
olegweb	Oleg Spitz	19	6	0	15	Feb 27th 2019	Feb 27th 2019
Marc	Mark Janson	3	0	2	2	Dec 8th 2021	Dec 8th 2021
Admin	Johanes Spencer	1	0	1	1	Nov 10th 2021	Nov 10th 2021
Caroline	Caroline Monte	3	0	0	2	Jan 28th 2022	Jan 24th 2022
Franz	Franz Ferdo	4	4	0	4	Aug 30th 2021	Dec 27th 2021
Mike	Michael Herring	9	2	3	7	Dec 8th 2021	Dec 8th 2021
jacob23	Jacob Ben	7	3	5	5	Jan 28th 2022	Jan 28th 2022
Greg	Gregory Shaw	3	0	3	3	Dec 8th 2021	Dec 8th 2021

Key benefits

01

Overview of access

Nanitor gives a clear overview of which of your users have what kind of access where, making it easier to identify weak points in your account setup.

02

Identify problems

Nanitor identifies accounts with problems that could pose risks to your system, such as users with no password set or expired passwords, accounts with admin access on multiple devices, or domain admin accounts on assets other than the domain controller.

03

Monitor activity

Discover potentially suspicious activity by seeing which users are currently logged in on which systems, when they were last active, and when they last logged on.

04

Clean up unused accounts

Nanitor helps you identify inactive user accounts that are no longer in use and should be locked or disabled.

Access to your systems should be tightly controlled

User accounts must be monitored closely, or they may become an attack vector into your organization's systems. An attacker who gains access to a user account on one system may be able to log into other systems accessible to the same user. A secure organization needs a clear overview of what each user can access and how, and must ensure accounts are secure.

Flexible technical policy

Different organizations have different needs. Nanitor allows you to decide for your organization which potential problems with user accounts become issues and how to prioritize them, reducing noise and ensuring the most pressing issues can be addressed first.

Confident user management

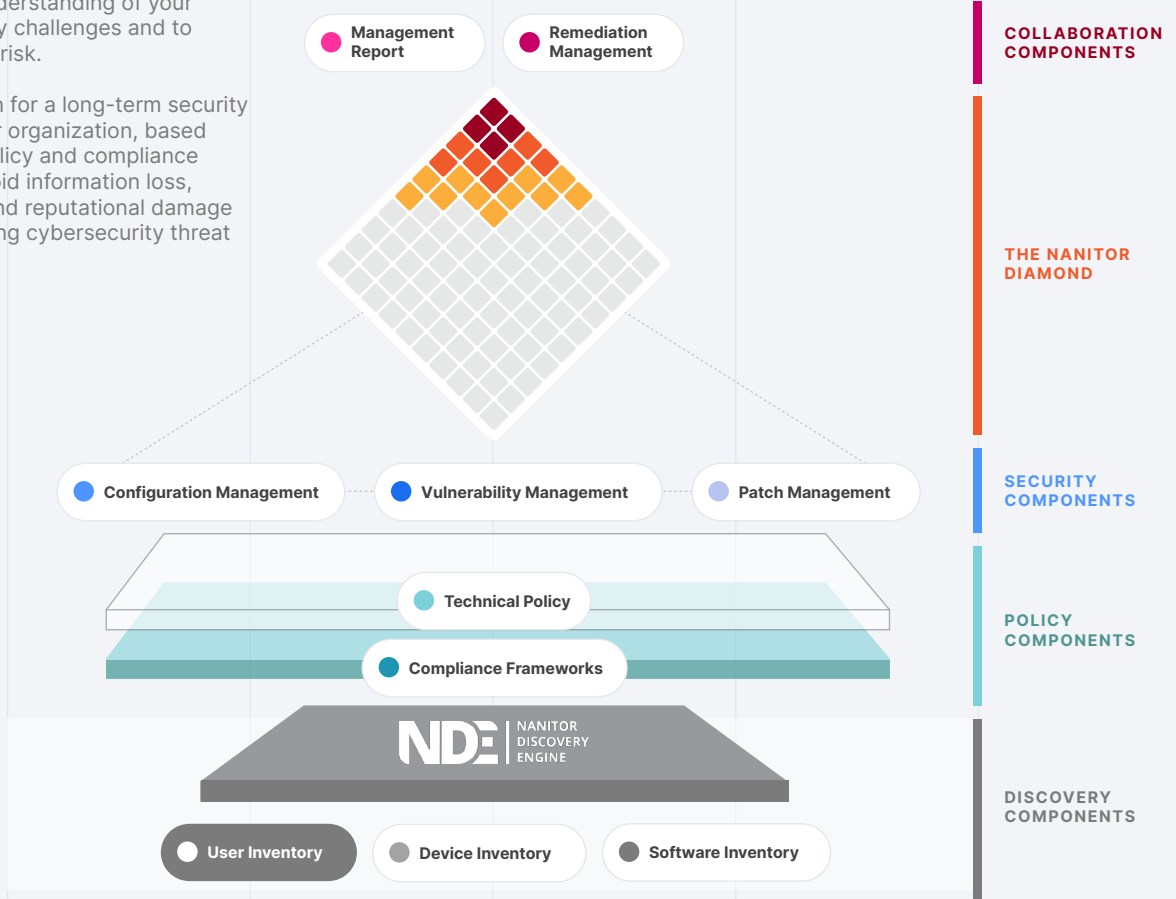
Nanitor's Discovery Engine™ collects information about user accounts on all of your assets. The lightweight, self-regulating agent runs invisibly in the background of your systems, monitoring in real time when users are active on which systems, what accounts exist, and any potential issues. The User Inventory shows all the data where you can sort and filter it, while potential issues are automatically consolidated and prioritized with other security issues in the Nanitor Diamond™.

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.

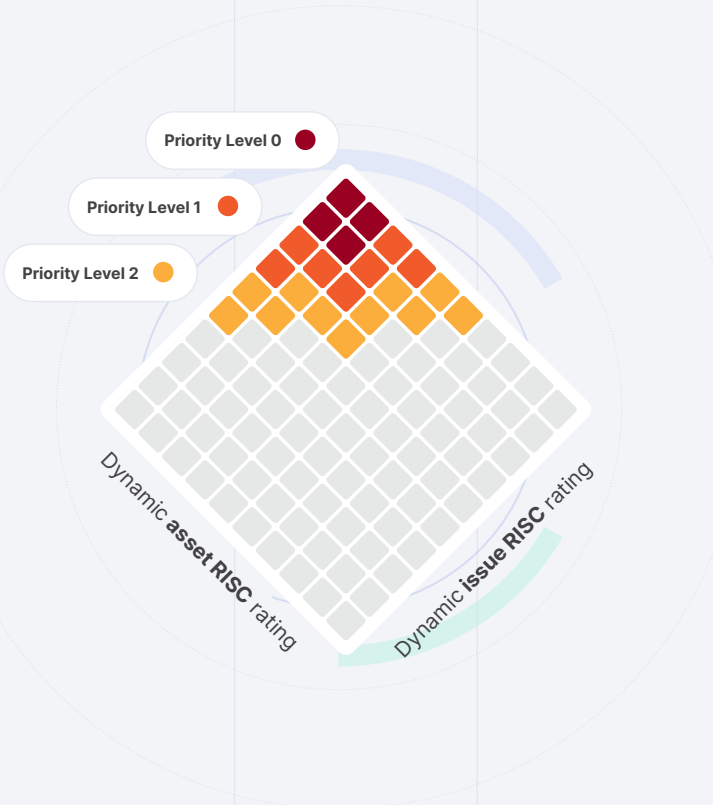


The Nanitor Diamond™

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.

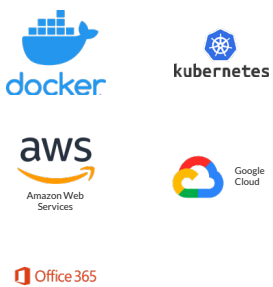
Employee workstations, servers and other assets can install the lightweight, cross-platform Nanitor Agent, an unobtrusive background process that monitors that asset and checks in to your Nanitor server with updates. Assets that cannot install software, such as network devices, can be monitored by the 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



Network Devices



Server



Desktop



Application Server



Application



Database

