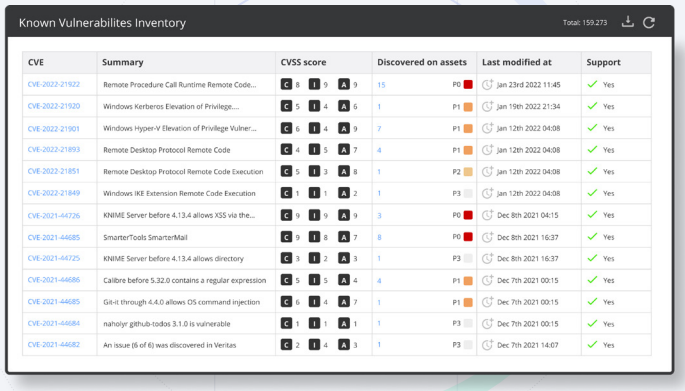
Nanitor

SECURITY COMPONENTS

Vulnerability Management

Stay up-to-date and aware of the known vulnerabilities in your infrastructure. Nanitor uses the latest information, including details from the NIST NVD (National Vulnerability Database), operating system vendors, respected vulnerability feeds as well as other industry sources. Nanitor is updated as required and searches for weaknesses in your infrastructure.



Key benefits

01
Automatic discovery

Nanitor continuously looks for known vulnerabilities in your infrastructure. Discovered vulnerabilities are automatically raised as security issues.

02
Prioritized view

Focused remediation. Discovered vulnerabilities are automatically prioritized, taking into account details of published severity, network exposure and potential impact in case of an exploit.

03
Current state overview

Using state-of-the-art algorithms, Nanitor makes sure that the vulnerability database is up to date. Our vulnerability feed includes details from a number of reputable sources, vendors and industry forums.

04
Detailed information

Vulnerabilities are identified and detailed information provided about what was identified, where it is located and how it may be remediated.

Vulnerabilities are a path to your important and sensitive data.

Attackers actively target IT infrastructures that are vulnerable to known exploits in order to breach them and access privileged information with malicious intent. Discovering and understanding what vulnerabilities exist in your environment supports your journey towards a better security posture.

The purpose of vulnerability management is to improve the security of your IT infrastructure by addressing known exploits and enssure ongoing compliance with your technical policy and regulatory requirements.

Automatically discover known vulnerabilties

Nanitor's lightweight, state-of-the-art vulnerability management engine equips cybersecurity teams with much needed detail about the state of their security landscape with continuous updates.

The recent critical **Apache Log4J / Log4Shell** vulnerability is prime example of where Nanitor quickly discovers and provides clear visibility to cybersecurity teams for quick remediation.

New vulnerabilities are raised every day

New vulnerabilities are raised every day and exploits are passed between attackers. With a state-of-the-art vulnerability engine and vulnerability feeds Nanitor continuously checks your IT infrastructure for known vulnerabilities and highlights the most critical ones.

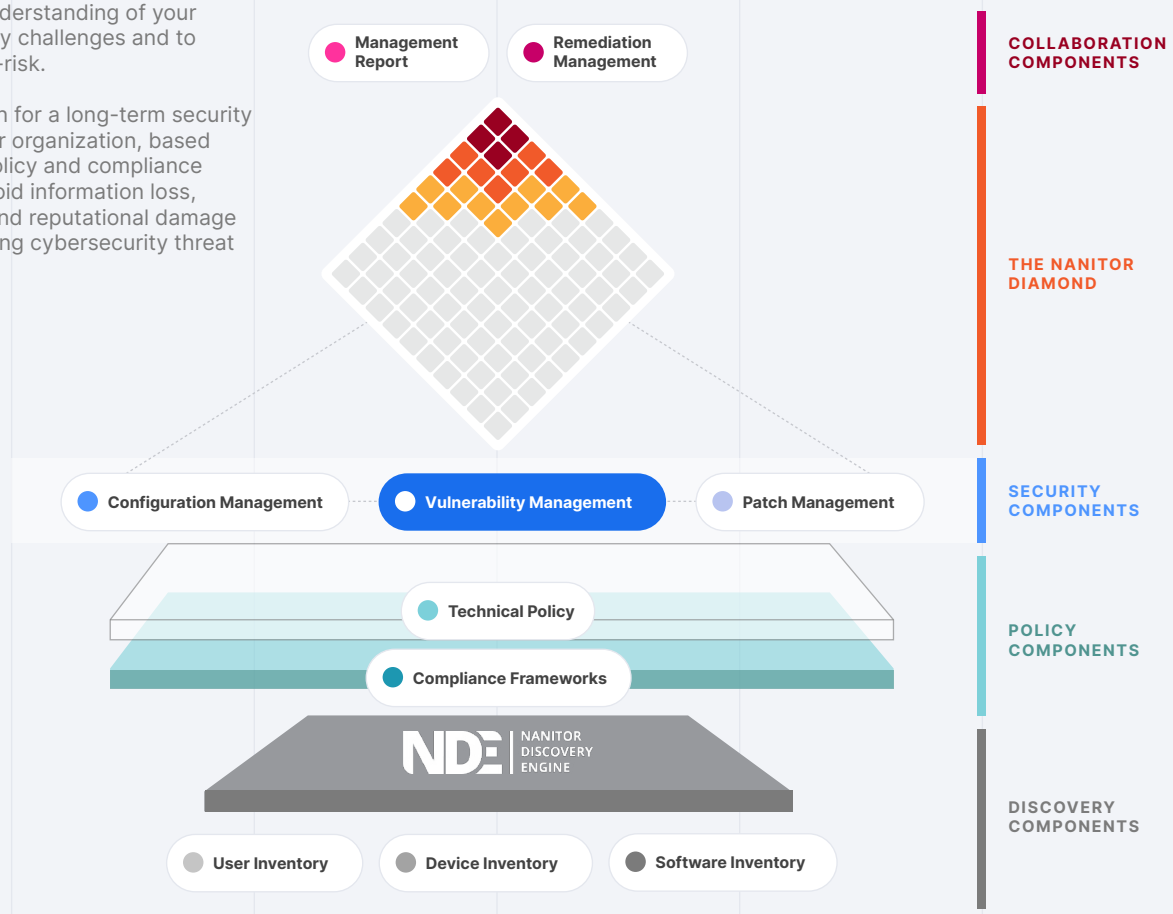
Equip yourself with real-time information about the status of your IT infrastructure with a proactive vulnerability management program and stay ahead of malicious attackers.

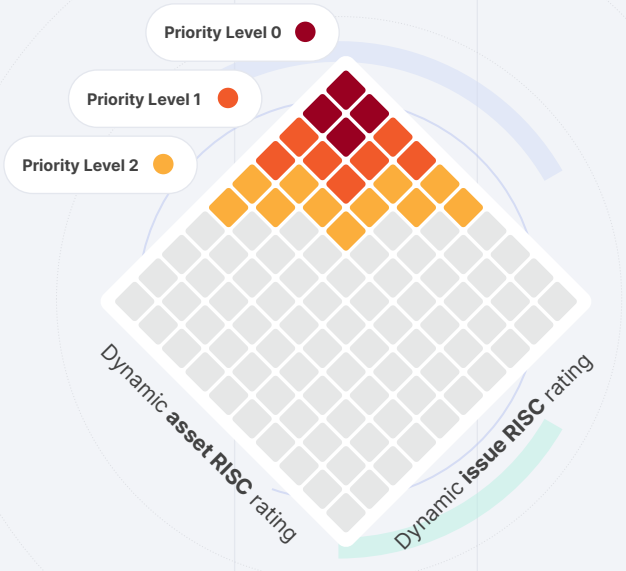
Learn more at: www.nanitor.com
Email: sales@nanitor.com

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