Nanitor

SECURITY COMPONENTS

# PII Endpoint Scanner

Protecting and controlling Personally Identifiable Information (PII) and avoiding accidental storage of it in unapproved locations is important to avoid potential data leakage.

Nanitor provides you with seamless detection of PII issues based on defined patterns such as credit card numbers, social security numbers and more.

When enabled, the Nanitor Agent automatically receives a binary that enables searching in common binary formats such as pdf, docx, xlsx, pptx in addition to text files such as .txt, .json, .xml, .log and more.

## Key benefits

01

### Quick time to result

Turning on the PII search only takes a few clicks and you can have your results up in minutes in a simple fashion.

02

### Low footprint

The PII search is designed to take minimal system resources and perfectly utilizes the NDE architecture to scan on specified systems over time. If the machine is restarted, it resumes where it left off.

03

### Reduce false positives

The Nanitor scanning mechanism uses various smart context-based methods in order to reduce false positives. Ignore lists can also be specified conveniently to filter out known test data.

04

### Focus your resources

By combining configuration and vulnerability information with data sensitivity, Nanitor can not only identify inappropriate data, but also identify the security compliance of involved assets. High-risk systems with sensitive data should receive immediate attention for addressing both PII issues and security posture.

## Vulnerable systems with sensitive data are at high risk for data leaks.

The unique combination of detection of PII issues with vulnerability, patch and configuration issues enables identifying the risk of data leakage which helps with prioritizing the key issues.
Ensuring that systems that are prone to data leakage are patched and securely configured helps reduce the chances of data being compromised.

## Lightweight operation for endpoints.

The PII Endpoint Scanner works on endpoint devices where the Nanitor Agent is installed. It is designed to run seamlessly in the background without bothering a user using the machine. When enabled on a device, the Nanitor Agent automatically downloads a supplementary PII binary that enables scanning binary file formats in addition to text file formats.

Once a PII issue is found, it is prioritized in the Nanitor Diamond and the system administrator is notified about it’s location in order to remediate the problem.

## Additional layer of protection - Avoid costly mistakes

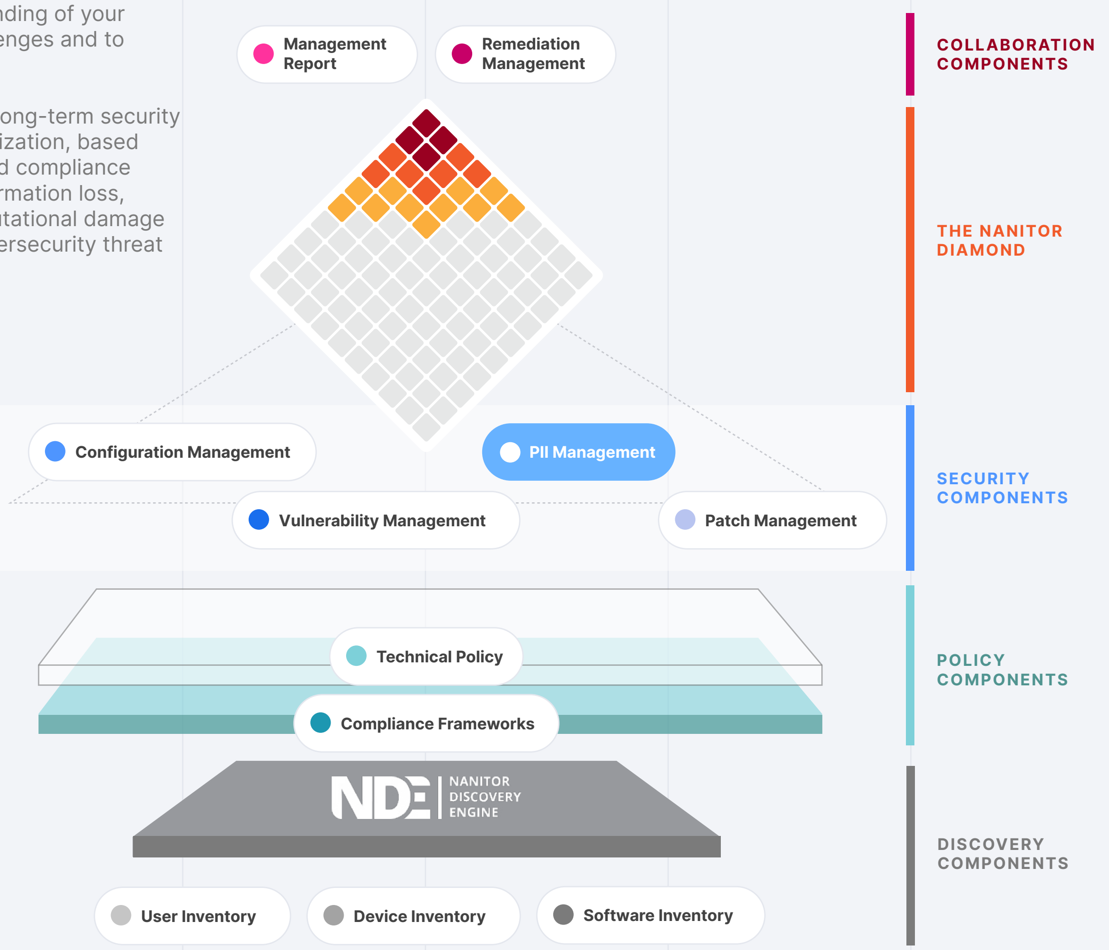
Most employees are just trying to do their job well. When interacting with customers, they might accidentally write down information they should not, or developers might test out application code with information they forgot to remove. Good processes can go a long way to eliminate such accidents, but it is important to catch what slips through the cracks. The Nanitor PII Endpoint Scanner is designed to help find those cases in a practical and efficient manner.

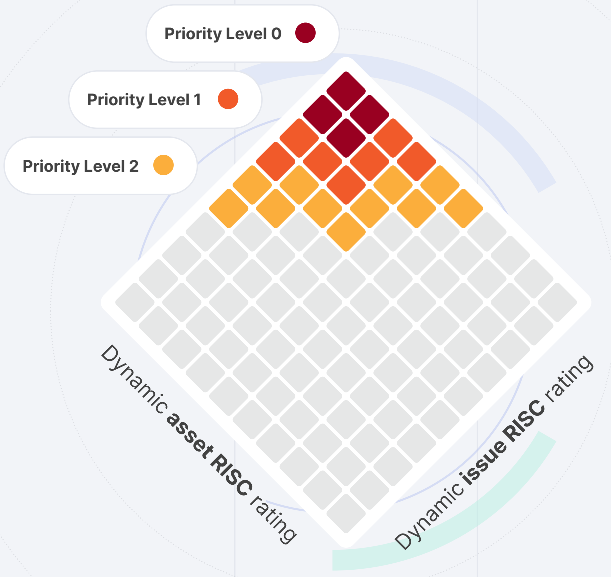
**Learn more at: www.nanitor.com**
**Email: sales@nanitor.com**

## 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
- Microsoft SQL Server