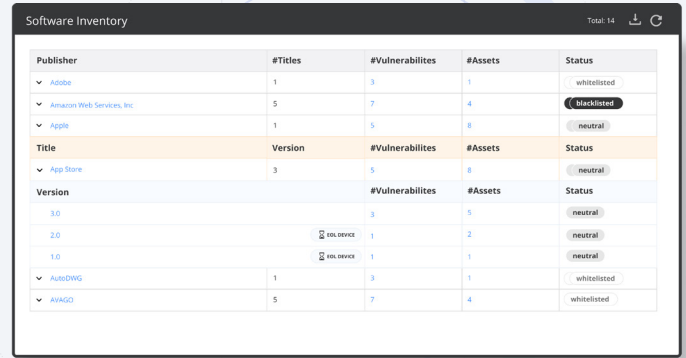


## DISCOVERY COMPONENTS

# Software Inventory

The Nanitor Software Inventory keeps track of what software is installed across your organization's assets. Quickly discover assets running outdated or vulnerable software, blacklist or whitelist specific software or software versions, or mark certain software as mandatory for a set of assets.



Publisher	#Titles	#Vulnerabilities	#Assets	Status
Adobe	1	3	1	whitelisted
Amazon Web Services, Inc.	5	7	4	blacklisted
Apple	1	5	8	neutral
Title	Version	#Vulnerabilities	#Assets	Status
App Store	3	5	8	neutral
	Version	#Vulnerabilities	#Assets	Status
	3.0	3	5	neutral
	2.0	1	2	neutral
	1.0	1	1	neutral
AutoDWG	1	3	1	whitelisted
AVAGO	5	7	4	whitelisted

## Key benefits

01

### Monitor software usage

Nanitor's Software Inventory gives a detailed overview of what software is installed on assets across the entire organization. See exactly which versions of any given software are in use on which assets.

02

### Identify vulnerable software

Nanitor lists known vulnerabilities on the specific software versions that are in use in your organization. Instantly see where software-based vulnerabilities exist and could be mitigated by updating or replacing vulnerable software.

03

### Blacklisting and whitelisting

Blacklist specific vendors, software titles or software versions to raise an issue whenever that software is detected on an asset - or choose a strict software policy, where any software not whitelisted will raise an issue. The scope of a rule can be organization-wide or apply to specific asset labels only.

04

### Mandatory software

Easily require installation of specific software on all assets, or all assets with particular labels, to automatically raise an issue for any asset that does not have the software installed.

## Vulnerabilities in installed software can leave an open door to attackers.

Installing and using different software is a necessary part of running any organization in the digital age, but all software, even trusted software, comes with risks. New vulnerabilities are discovered in widely used software every day, and while software vendors may release patches, old and unpatched versions of the software often remain installed and in use for years after the vulnerability has been published.

For security, it is critical to track potentially vulnerable software in use across an organization and ensure it is patched or replaced before the vulnerability can be exploited by malicious actors.

## Powerful software policy management

Choose between a soft policy, where only blacklisted software and missing mandatory software will raise issues, or a detailed policy, where any software that is not explicitly whitelisted or mandatory will raise an issue. The flexible rule engine allows complex combinations of rules that interact in an intuitive way, such as blacklisting a software title across the organization but whitelisting it for a particular asset label, or making a title mandatory but blacklisting certain versions known to be vulnerable.

## Detailed overview of software

Nanitor's Discovery Engine collects information on all software installed on your organization's assets and securely checks it in to your organization's central Nanitor instance. There, the software inventory data is cross-referenced with Nanitor's rules for whitelisted, blacklisted and mandatory software for the given asset, as well as a database of known vulnerabilities, and appropriate issues are raised and prioritized.

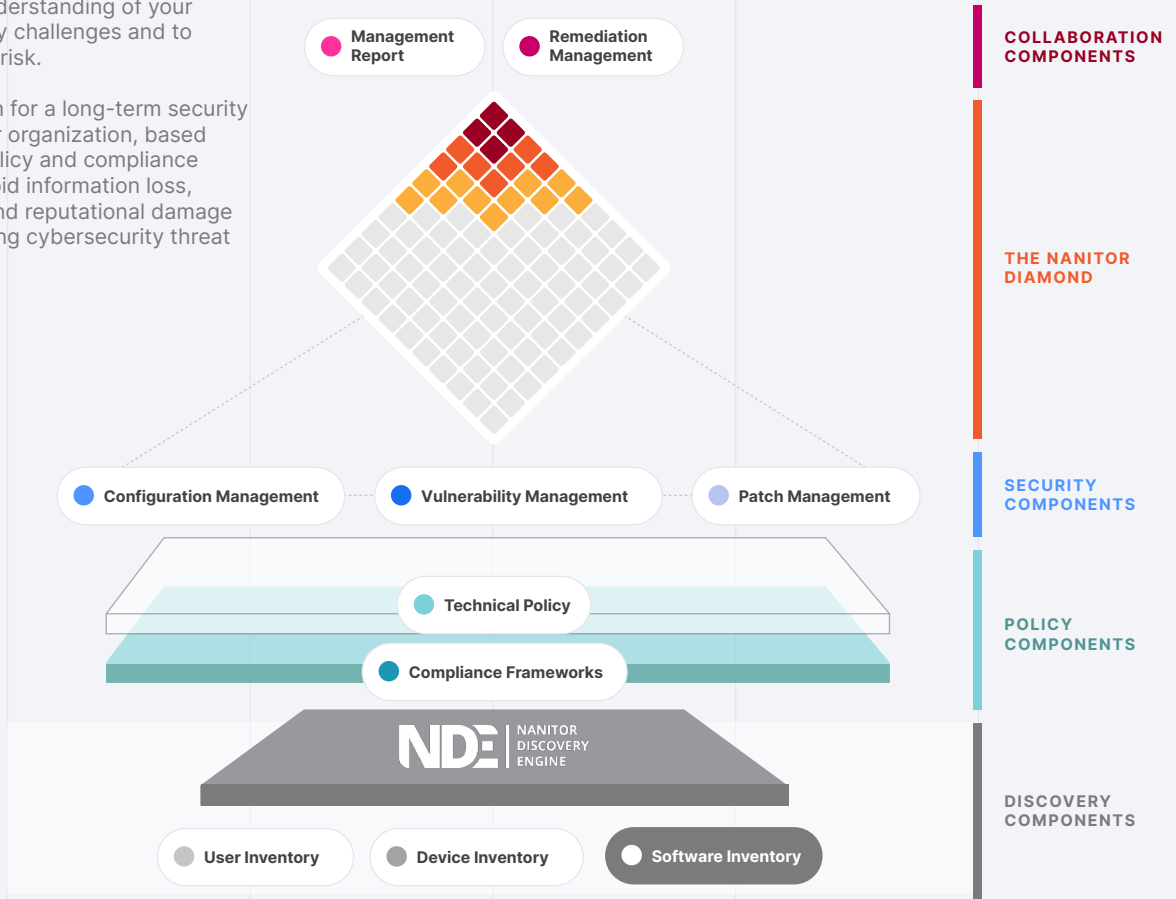
The Software Inventory provides a searchable overview of all software installed across the organization, where you can drill down into individual vendors, titles or software versions for what assets have them installed and what vulnerabilities are associated with them.

Learn more at: [www.nanitor.com](http://www.nanitor.com)  
Email: [sales@nanitor.com](mailto: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.

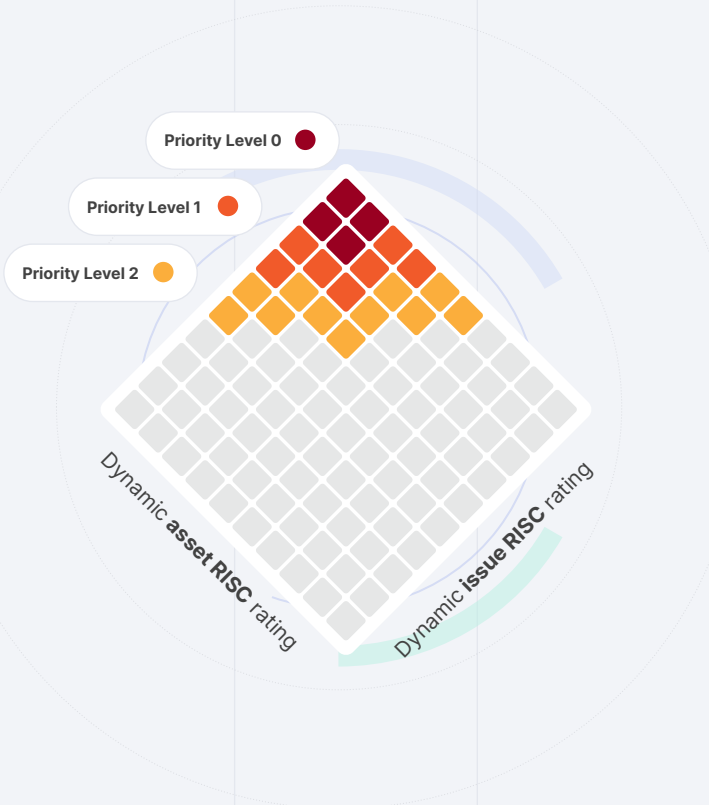


## The Nanitor Diamond™

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.

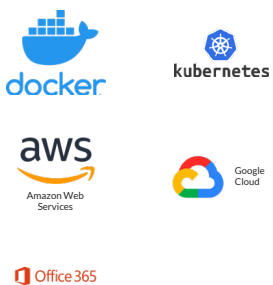
Employee workstations, servers and other assets can install the lightweight, cross-platform Nanitor Agent, an unobtrusive background process that monitors that asset and checks in to your Nanitor server with updates. Assets that cannot install software, such as network devices, can be monitored by the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

