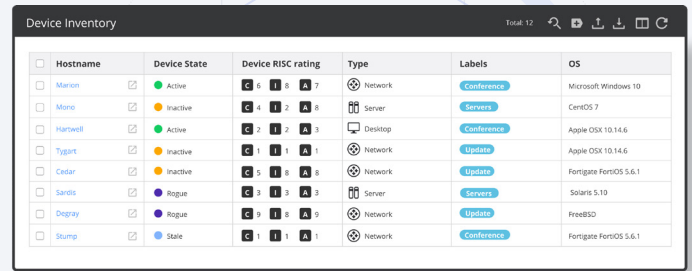


## DISCOVERY COMPONENTS

# Device Inventory

The Nanitor Device Inventory contains essential real-time information about your organization's assets in a flexible, searchable and filterable format. Check the status of your assets or a given asset and view information such as compliance scores, issues detected, missing patches, user accounts, software, open ports, or recent activity.



Hostname	Device State	Device RISC rating	Type	Labels	OS
Marion	Active	C 6 I 8 A 7	Network	Conference	Microsoft Windows 10
Mono	Inactive	C 4 I 2 A 8	Server	Servers	CentOS 7
Hartwell	Active	C 2 I 2 A 3	Desktop	Conference	Apple OSX 10.14.6
Tygart	Inactive	C 1 I 1 A 1	Network	Update	Apple OSX 10.14.6
Cedar	Inactive	C 5 I 8 A 8	Network	Update	Fortigate FortiOS 5.6.1
Sandis	Rogue	C 3 I 3 A 3	Server	Servers	Solaris 5.10
Degray	Rogue	C 9 I 8 A 9	Network	Update	FreeBSD
Skump	Stale	C 1 I 1 A 1	Network	Conference	Fortigate FortiOS 5.6.1

## Key benefits

### 01

#### All your assets in one place

See information about all of your assets in one sortable list: servers, workstations, databases, network devices, or other assets. Quickly filter on assets with: outstanding issues, out-of-date Nanitor agents, end-of-life operating systems, and more. Ensure every asset is checking in as it should.

### 02

#### Security status on every asset

View detailed information on your assets, their current status and history, and any issues that affect them. Benchmark scores, patch status, users, installed software, ports and networking, and an activity log of security-related events affecting this asset are easily accessible.

### 03

#### Detect unexpected assets

Find and tease out unmonitored assets connected to your organization's network (rogue), assets that have stopped checking in but remain on the network (stale), or assets that continue to check in via the Nanitor Agent after being decommissioned (ghost).

### 04

#### Manage and organize assets

Through Nanitor's interface, assets can be labeled manually or automatically in the system based on customized rules, marked as decommissioned to raise an issue on any subsequent checkin. Agent upgrades can be requested, without logging in to each individual asset.

## Every asset with access to company data can be a liability if not monitored for security issues.

Attackers can slip into the system through a security vulnerability on just one machine. Keeping track of every asset currently or formerly in use at an organization is an ever-growing task, and without thorough monitoring, something can easily slip through the cracks.

Maintaining a complete overview of all relevant assets and potential security problems affecting them is vital to securing your organization against threats.

## Flexible organization of assets

Set up automatic rules to label your assets based on hostname patterns, subnets, platforms, or OUs, or apply labels manually where necessary.

Rate the importance of different asset labels or individual assets on the Confidentiality Integrity Availability scale, according to your organization's needs and priorities. Many features can be enabled or disabled for particular asset labels for maximum flexibility.

## Analyzing your assets in real time

Nanitor's Discovery Engine collects a wealth of information on each of your assets that could impact security: benchmarks scores, installed and missing patches, user accounts, software, open ports, subnets, and more. The complete overview of the status of your assets is easily accessible through the Nanitor interface, with filtering, searching and sorting capabilities. Security issues are raised as soon as they are discovered, and are viewable for each asset individually or prioritized across the entire organization, to be reviewed and remediated by your security team.

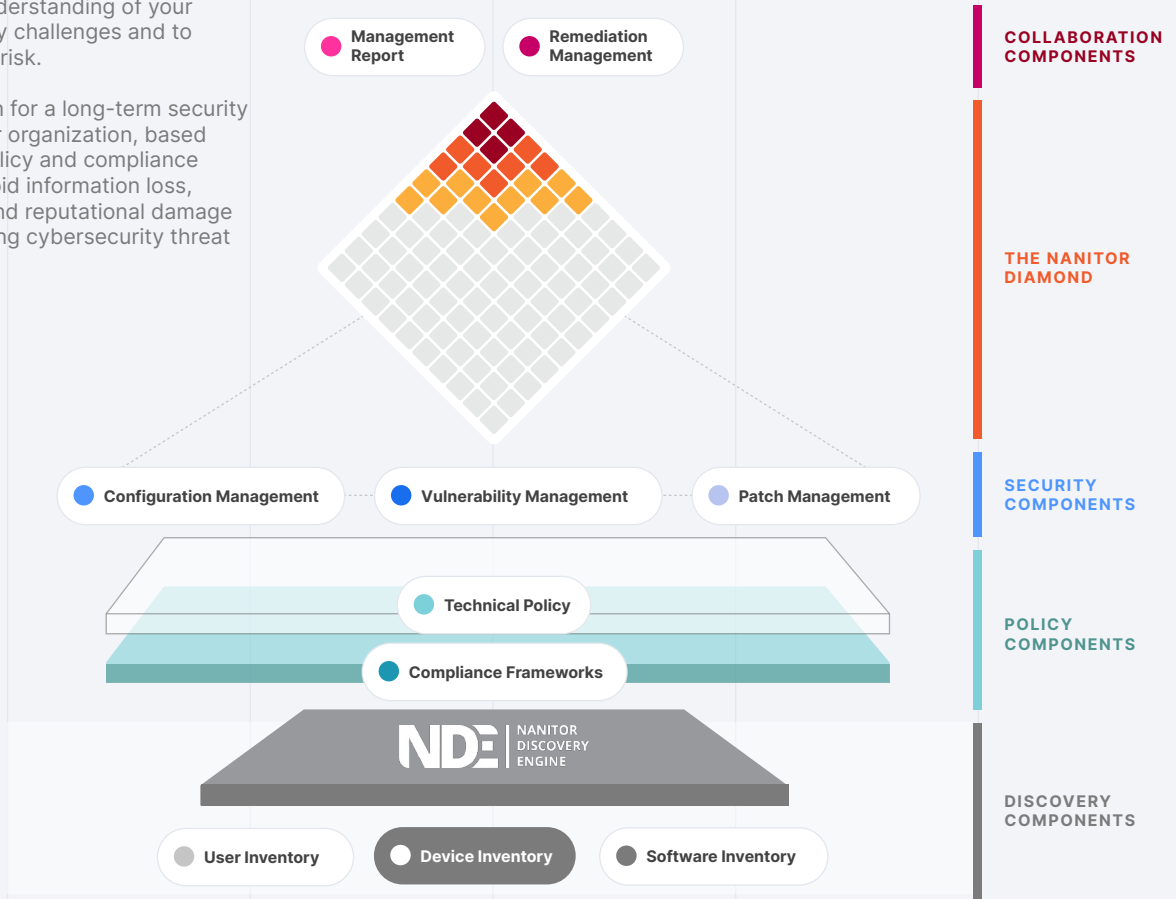
By enabling Network Discovery, Nanitor can discover devices on the network even if they have not installed the Nanitor Agent or been registered with the Nanitor Collector. Assets are flagged if they are unmonitored (rogue), have gone inactive (inactive), are still found on the network but no longer checking in (stale), or are decommissioned but still checking in (ghost).

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.

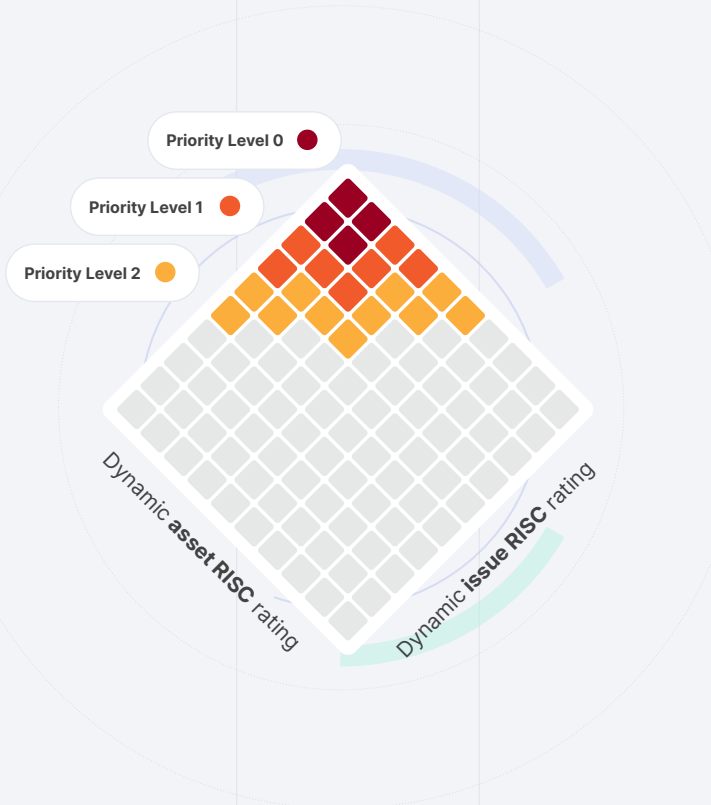


## The Nanitor Diamond™

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.

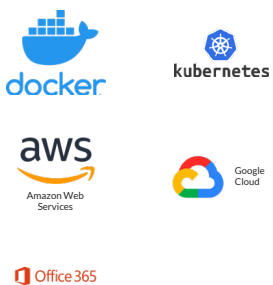
Employee workstations, servers and other assets can install the lightweight, cross-platform Nanitor Agent, an unobtrusive background process that monitors that asset and checks in to your Nanitor server with updates. Assets that cannot install software, such as network devices, can be monitored by the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

