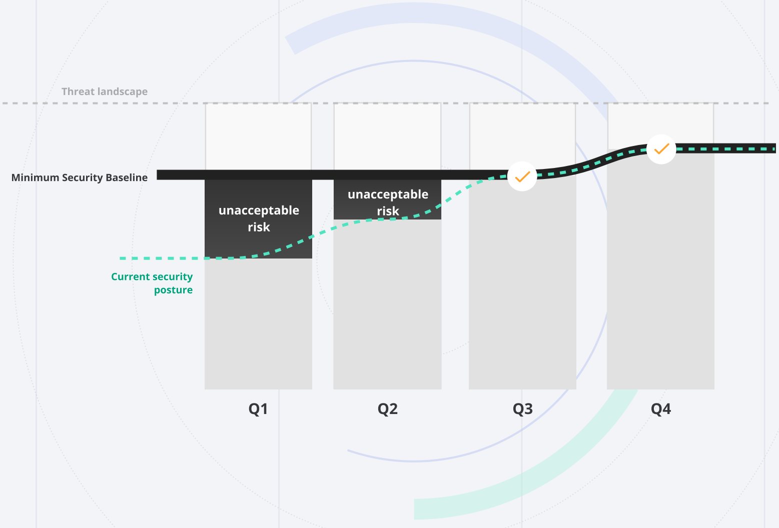
POLICY COMPONENTS

# Technical Policy

Nanitor's Technical Policy Management supports building organizational consensus around your cybersecurity strategy.

Your approved goals and rule definitions are articulated in your security baseline settings so that you can focus on what's important in terms of minimizing risk.



## Key benefits

### 01
### Flexibility

Nanitor supports your technical policy creation with built-in support for benchmarks based on CIS and NIST recommendations and is guided by compliance frameworks (e.g. ISO 27001, PCI DSS and others). You decide your security baseline.

### 02
### Collaboration

With centralized management of cybersecurity policies and rules with integrated detailed descriptions and remediation support, Nanitor enables effective team-collaboration.

### 03
### Best Practices

Nanitor supports your journey towards secure by default with industry best-practices and compliance frameworks built into the platform, assisting you with enforcement of your technical policy.

### 04
### Security Policy Assurance

Issue remediations are automatically detected and linked to your policy decisions, reflecting high-level decisions about risk management and rule enforcement. With Nanitor, your security posture is monitored and updated in real time.

## Assisting your security objectives

Managing your cybersecurity strategy and aligning with compliance frameworks, recognized best practices and company requirements can be a difficult and expensive task.

Challenges include:

- building consensus around security strategies
- sourcing and using industry best practices
- setting security baseline according to acceptable risk
- enforcing rules accross all assets
- documentation of security policy.

The Nanitor Technical Policy component supports your efforts with all of the above and much more.

✓ **Maintain a comprehensive inventory of your IT assets**

✓ **Document and enforce risk as part of your cybersecurity program.**

✓ **Accurately assess criticality of assets and ensure you focus on the top priority.**

## Define your Technical Policy

Decide how to address cybersecurity requirements in Nanitor based on best-practices, compliance frameworks and company-approved policies.

Nanitor supports and drives effective collaboration with stakeholders on your technical policy and enables conscious decisions regarding your cybersecurity strategy.

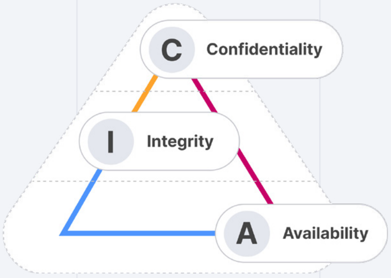
**In Nanitor your Technical Policy addresses:**

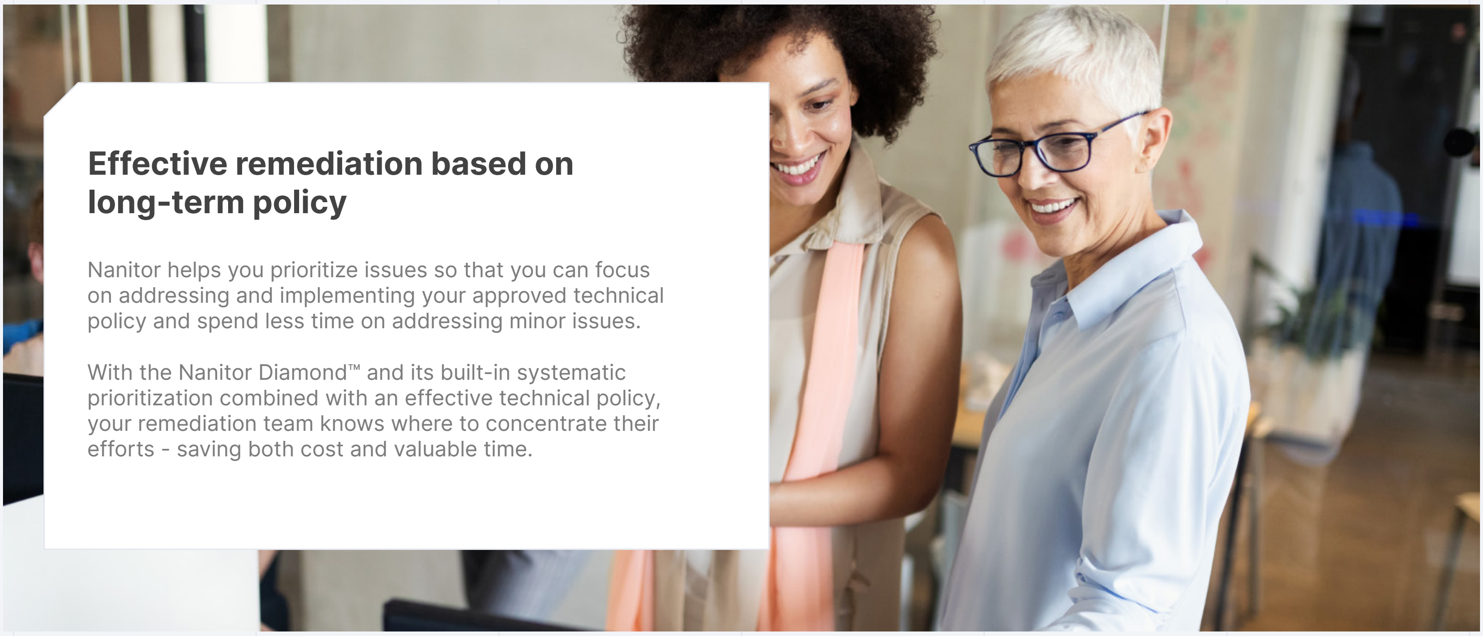
- ✓ Security configurations
- ✓ Known vulnerabilities
- ✓ Security patches
- ✓ User privileges
- ✓ Software policy
- ✓ Asset detection
- ✓ End-of-life asset management

## Manage asset risk

Nanitor supports automatic application of risk assessment rules in your environment, assigning risk ratings to your assets using the established Confidentiality Intergrity Availability triad.

With Nanitor, you manage and document your asset risk inside the Nanitor platform. Automatic risk adjustment taking into account asset risk across the organization as well as the risk posed by different issues ensures that your focus stays on your most critical issues while maintaining complete real-time visibility.





## Effective remediation based on long-term policy

Nanitor helps you prioritize issues so that you can focus on addressing and implementing your approved technical policy and spend less time on addressing minor issues.

With the Nanitor Diamond™ and its built-in systematic prioritization combined with an effective technical policy, your remediation team knows where to concentrate their efforts - saving both cost and valuable time.

## What is Nanitor?

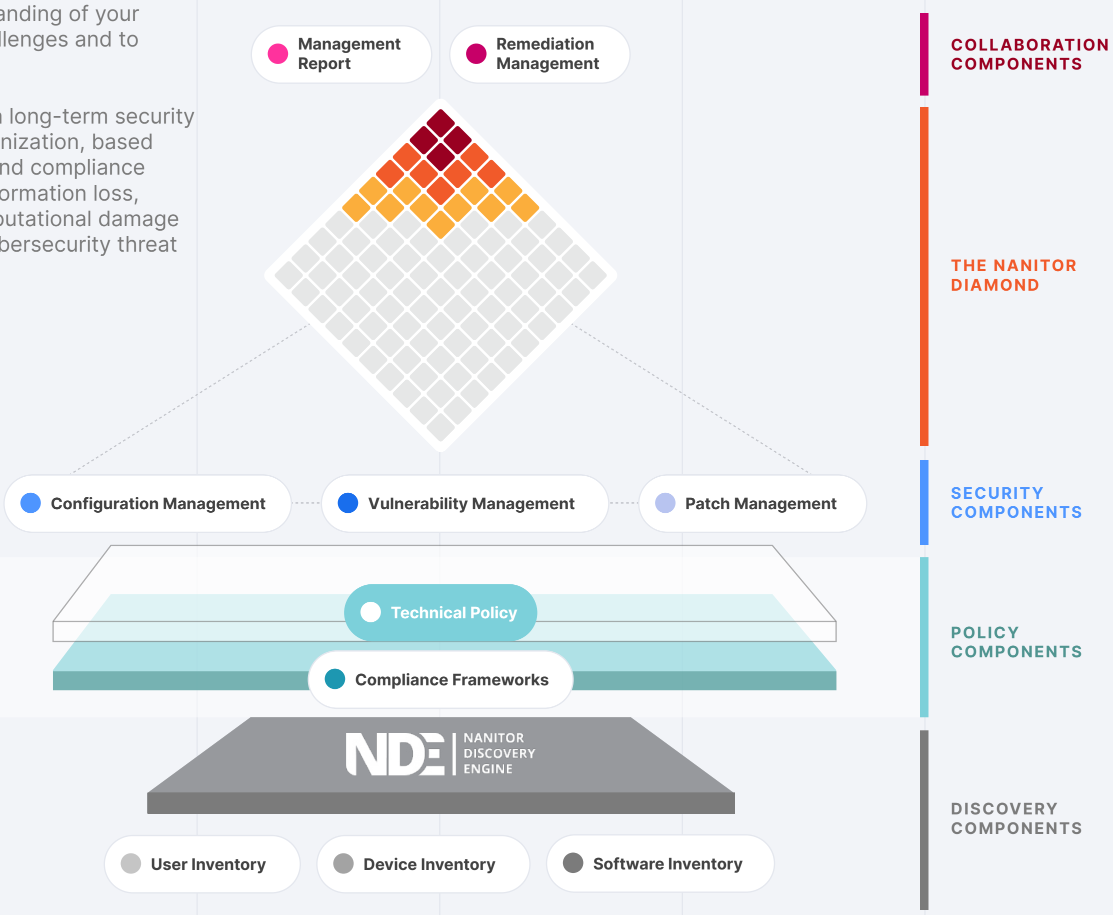
Nanitor is a powerful cybersecurity management platform focusing on hardening security fundamentals across your global IT infrastructure. The platform provides unique visibility and control of your security challenges that stakeholders can trust, at a fraction of the cost and time of alternatives.

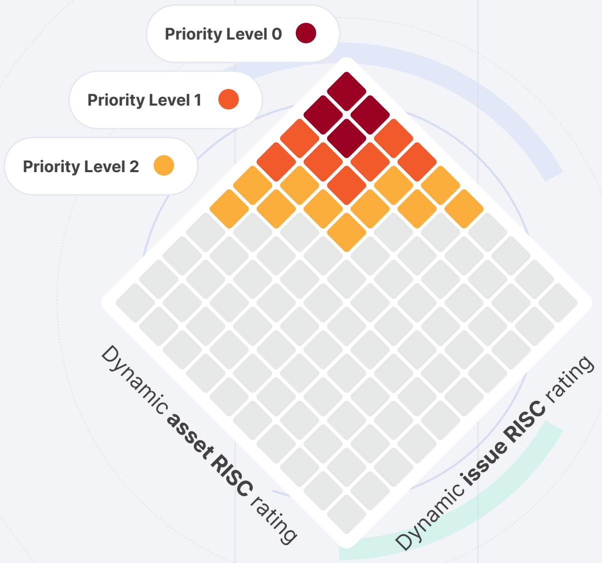
**Learn more at: www.nanitor.com**
**Email: sales@nanitor.com**

## 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 networks
UBIQUITI networks
Check Point Software Technologies Ltd
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

N Nginx
Microsoft IIS
Exchange

### Application

Chrome
Internet Explorer
Microsoft Office

### Database

MySQL
ORACLE DATABASE
PostgreSQL
Microsoft SQL Server