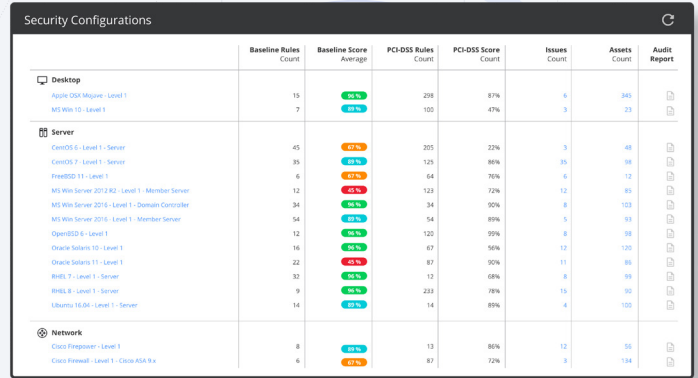


**SECURITY COMPONENTS**

# Configuration Management

One of the fundamentals of building a solid Cyber Security strategy is knowing what devices and applications are in use and how they are configured in terms of security.

Nanitor provides you with real-time visibility of potential issues with your security configuration, helping you to focus your hardening efforts.



	Baseline Rules Count	Baseline Score Average	PCI-DSS Rules Count	PCI-DSS Score Count	Issues Count	Assets Count	Audit Report
<b>Desktop</b>							
Apple OSX Mojave - Level 1	15	100%	298	87%	6	345	
MS Win 10 - Level 1	9	100%	105	47%	3	23	
<b>Server</b>							
CentOS 6 - Level 1 - Server	45	87%	205	22%	3	48	
CentOS 7 - Level 1 - Server	35	89%	125	86%	35	98	
FreeBSD 11 - Level 1	6	42%	64	76%	6	12	
MS Win Server 2012 R2 - Level 1 - Member Server	12	45%	123	72%	12	85	
MS Win Server 2012 - Level 1 - Domain Controller	34	85%	34	30%	8	103	
MS Win Server 2016 - Level 1 - Member Server	54	89%	54	60%	5	15	
OpenBSD 6 - Level 1	12	95%	120	39%	8	38	
Oracle Solaris 10 - Level 1	16	95%	67	56%	12	125	
Oracle Solaris 11 - Level 1	22	45%	87	30%	11	86	
RedEL 7 - Level 1 - Server	32	95%	12	68%	8	99	
RedEL 8 - Level 1 - Server	9	95%	233	78%	15	90	
Ubuntu 16.04 - Level 1 - Server	14	89%	14	89%	4	100	
<b>Network</b>							
Cisco Firepower - Level 1	8	82%	13	86%	12	55	
Cisco Firewall - Level 1 - Cisco ASA 9.8	6	87%	87	72%	8	134	

## Key benefits

**01**

### Reduce the attack surface

Ensuring that security configurations follow best practices helps create a strong first line of defense in order to reduce the blast radius in case a malicious user gains access to your systems.

**02**

### Complete visibility

Nanitor's intuitive user interface gives a comprehensive picture of current security configurations and, in combination with the Technical Policy component, makes it easy to create a risk reduction program.

**03**

### Integrated use of industry best practices

Nanitor tracks the security posture of your systems and ensures that they follow your technical policy. When insecure configurations are detected, Nanitor will provide detailed information and prioritization along with remediation instructions.

**04**

### Quick time-to-result

Ensuring that security configurations follow best practices helps create a strong first line of defense in order to reduce the blast radius in case a malicious user gains access to your systems.

## Security does not happen by chance.

Security must be consciously designed, implemented and enforced.

Out-of-the-box configurations for IT assets focus on ease-of-use and often favor simplicity over security. Many computer systems are insecure by default, allowing malicious users to roam freely around your network when they get through basic defenses.

Configuring your assets according to best practices is a fundamental security requirement and an essential line of defense against threats.

## Configuration based on best practices

The Nanitor Configuration Management component provides comprehensive visibility of your security configurations across all platforms, enabling effective management of your security technical policy.

This makes it easy to detect and remediate configuration issues. After defining your technical policy and compliance requirements, your organization can track violations of the policy in real time through Nanitor, with detailed remediation instructions where rules are broken.

## Key functionality

- ✓ Nanitor maintains a comprehensive inventory of all your assets, applications, services, users and networks.
- ✓ Define and document your organization's technical policy within the Nanitor system in accordance with on proven industry best practices, compliance frameworks and regulatory requirements.
- ✓ Once your technical policy is defined, Nanitor helps your organization enforce it by compiling, listing and prioritizing potential violations of the policy in the configuration of your systems. Each issue comes with detailed remediation instructions.
- ✓ Nanitor can generate printable reports on potential issues for security officers and management, providing an overview of your organization's security status.
- ✓ Organize important issues into Projects within the Nanitor system and assign them to relevant staff, then track progress on remediating the issues as you tighten up your systems.

01

### Industry best practices

**NIST**

**CYBER  
ESSENTIALS**

**CIS** Center for  
Internet Security

02

### Compliance frameworks

- ✓ ISO 27001
- ✓ PCI
- ✓ HIPAA
- ✓ SOC2

03

### Regulatory requirements

- ✓ NIS - Network and Information Systems
- ✓ National Infrastructure Directive

## What is Nanitor?

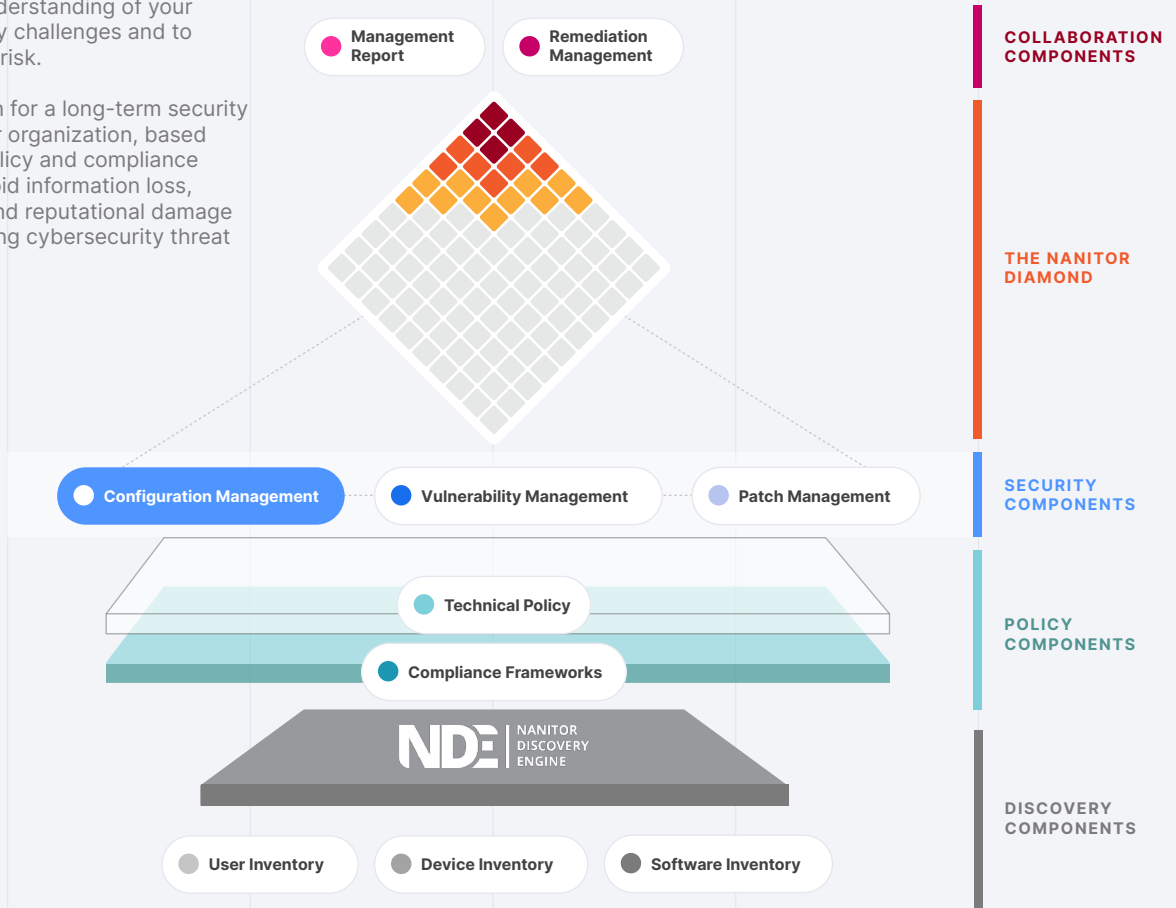
Nanitor is a powerful cybersecurity management platform focusing on hardening security fundamentals across your global IT infrastructure. The platform provides unique visibility and control of your security challenges that stakeholders can trust, at a fraction of the cost and time of alternatives.

**Learn more at: [www.nanitor.com](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.

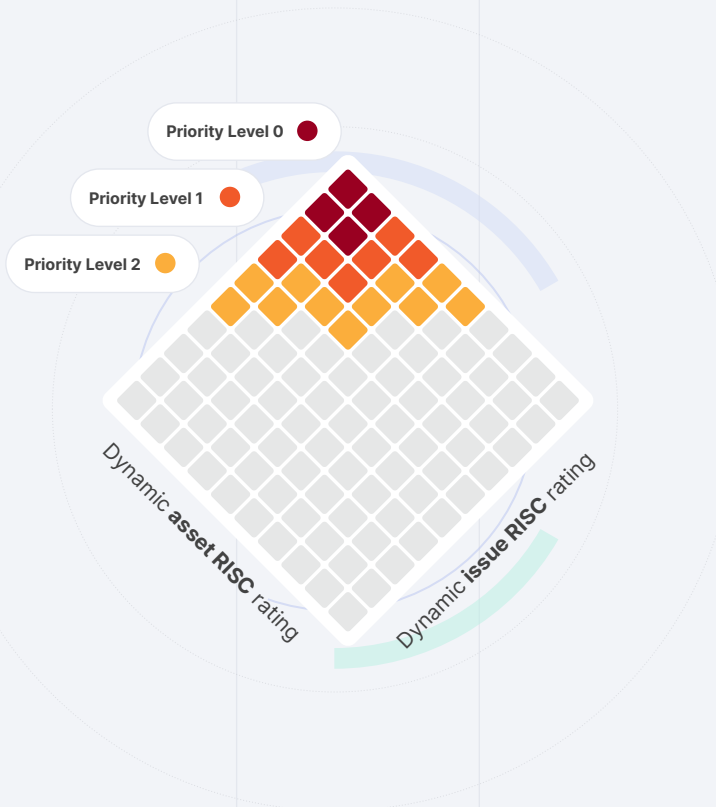


## The Nanitor Diamond™

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