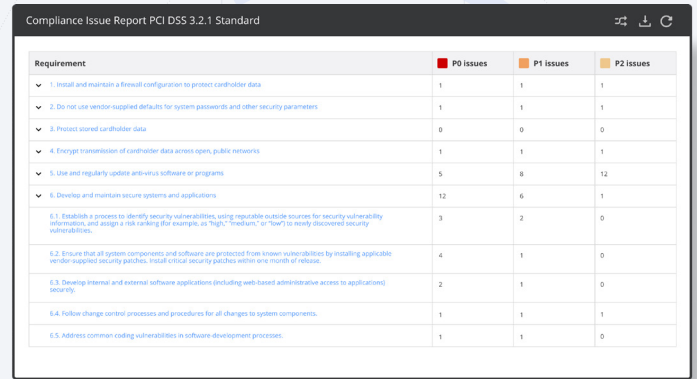


POLICY COMPONENTS

Compliance Frameworks

The Nanitor Compliance Framework Support provides the capability to match your Technical Policy with your necessary compliance requirements and best practices. Devise a policy for your organization that is in line with compliance standards and works for you.



Requirement	PO issues	P1 issues	P2 issues
1. Install and maintain a firewall configuration to protect cardholder data	1	1	1
2. Do not use vendor-supplied defaults for system passwords and other security parameters	1	1	1
3. Protect stored cardholder data	0	0	0
4. Encrypt transmission of cardholder data across open, public networks	1	1	1
5. Use and regularly update anti-virus software or programs	5	8	12
6. Develop and maintain secure systems and applications	12	6	1
6.1. Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, "high," "medium," or "low") to newly discovered security vulnerabilities	3	2	0
6.2. Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches, install critical security patches within one month of release	4	1	0
6.3. Develop internal and external software applications (including web-based administrative access to applications) securely	2	1	0
6.4. Follow change control processes and procedures for all changes to system components	1	1	1
6.5. Address common coding vulnerabilities in software development processes	1	1	0

Key benefits

01

Large set of frameworks

Includes support for compliance and industry best practice frameworks such as PCI-DSS, ISO27001, NIST CSF, NIST 800-53, CIS Controls and more.

02

Compliance-based overview

The Compliance Overview page provides a clear view of how you stand in each Control/Requirement and shows clearly where you need to improve.

03

Alignment

Alignment of your Technical Policy with best practices and regulatory compliance helps getting the team on the same page and aligned for success.

04

Automation

Nanitor automatically checks and reports on thousands of compliance-related security issues across your infrastructure.

Compliance frameworks and best practices are hard to do well

Checking and fulfilling cybersecurity compliance requirements is tricky. In practice, checks are often made on small sample sizes as a best effort since checking individual settings on a large set of devices is cumbersome and time-consuming work.

Tracking changes over time is another gigantic task that is not feasible without proper automation.

Alignment of key stakeholders

With the entire team viewing a clearly defined Technical Policy as matching up with your Compliance Framework, change history and comments enables your team to have clear visibility and team communication enables a common understanding and a platform to track changes and make decisions. This also makes it easy to demonstrate status and progress to auditors.

Detailed overview of compliance and gaps

The Nanitor Discovery Engine automatically connects each discovered issue with compliance framework controls based on issue type and nature of the issue.

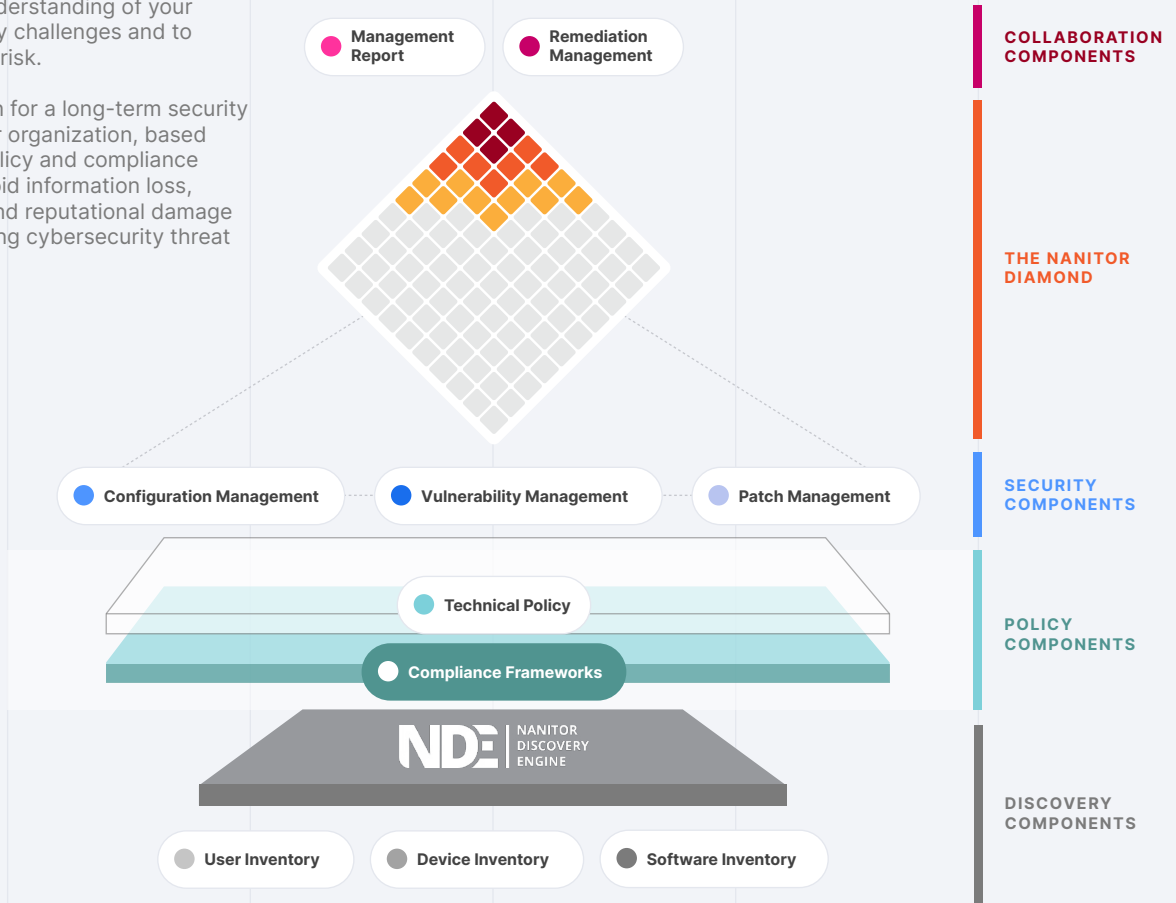
This enables you to see what controls Nanitor covers, and what issues and checks are under each control. Furthermore, the issues are also prioritized based on RISC prioritization for effective remediation.

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.

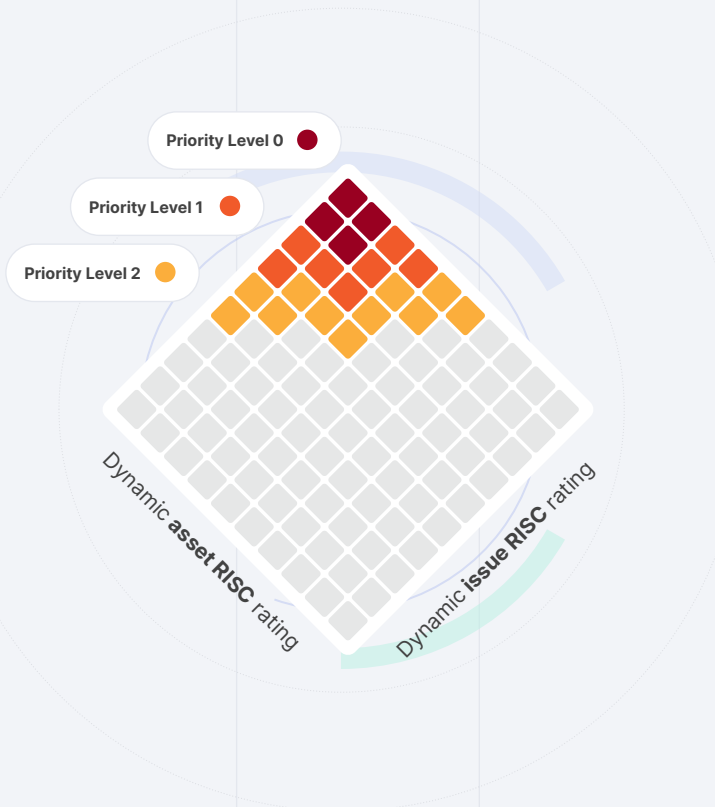


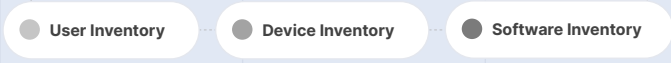
The Nanitor Diamond™

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.





- ✓ 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

