Natroy Compliance: Real-Time Policy Enforcement & CVE Monitoring

Executive Summary

Natroy Compliance is the policy enforcement and security posture management module within the Natroy platform. It continuously monitors infrastructure for configuration drift, security vulnerabilities (CVEs), and policy violations turning compliance from a static report into a dynamic, actionable discipline.

The module gives compliance, security, and infrastructure teams a unified, real-time view of risks across their environment. It connects violations directly to remediation (via Natroy O) or escalation workflows (via Natroy I), enabling organizations to stay audit-ready and proactively secure.

Module Description

Natroy Compliance is designed to reduce the complexity of understanding and resolving compliance violations. With support from Natroy X, users don’t need to manually interpret each vulnerability. The system automatically determines which CVEs impact your infrastructure, provides explanation and severity context, proposes possible workarounds or fixes, and assists in building automation templates using Natroy O.

Once detected, incidents can be closed manually or through automated workflows governed with full ITIL-compliant ticketing and approval processes.

The module monitors devices, services, and configurations discovered by Natroy T and evaluates them against customizable rules for protocol use, firmware versions, software lifecycle, and known CVEs.

Policy rules are applied by device type, tag, vendor, region, or function enabling fine-grained control across multi-vendor networks. Violations are detected instantly, visualized on dashboards, and linked to automated or ticket-based resolution.

Core Functionality

1. Policy Rule Engine
   - Create policies for SNMP/SSH usage, insecure services, end-of-life firmware, and more
   - Apply by topology group, site, or business role
   - Leverage built-in templates or customize per environment
2. CVE Intelligence Matching
   - Pull CVE data from public sources and vendor APIs
   - Automatically detect which vulnerabilities actually impact your infrastructure
   - Organize real threats by affected device, version, and severity
   - Eliminate thousands of false positives that overwhelm teams
3. Compliance Dashboards & Risk Maps
   - Score compliance per site, device, policy type, or vendor
   - Highlight high-risk infrastructure areas
   - Drill down into each violation's context, state, and history
4. Audit & Reporting Tools
   - Export full violation history with resolution timelines
   - Generate compliance evidence for SOC2, ISO27001, NIST
   - Track SLA compliance and recurring nonconformities
5. Response Integration
   - Auto-open incidents in Natroy I or ServiceNow
   - Launch automated fixes via Natroy O (e.g., disable SNMPv1)
   - Mark exemptions or partial remediation status

Architecture & Security

- Stateless engine using feeds from Natroy T
- Container-based, horizontally scalable
- RBAC and policy scoping by role and business domain
- Full encryption in motion and at rest

Use Cases

- Real-time CVE scanning and exposure management
- Automated enforcement of secure protocol standards
- Lifecycle policy enforcement (firmware, OS, vendor end-of-support)
- Audit preparation with downloadable logs and evidence
- SLA visibility into compliance issue response

AI-Ready with Natroy X

- Predict likely violations based on asset behavior
- Auto-prioritize risk remediation by exposure and function
- Recommend new policies based on peer benchmarking

Before vs. After Natroy Compliance

Capability	Before Natroy Compliance	With Natroy Compliance
Policy Enforcement	Manual reviews, inconsistent checks	Real-time, automated checks using prebuilt best practices
CVE Awareness	Generic feeds, manual interpretation	Automatic interpretation and impact analysis with Natroy X
False Positive Management	Thousands of irrelevant alerts	Only actionable CVEs based on your infrastructure
Remediation Lifecycle	Disconnected tools, manual fixes	Detection Ticket Approval Automated Fix (via Natroy I + O)
Audit Preparation	Spreadsheet-based, time-intensive	One-click reporting with resolution logs and SLA history
Governance & Control	Email threads, unclear ownership	ITIL-aligned ticketing, workflow approvals, and audit traceability
Best Practice Validation	Unclear standards, manual review	Built-in network and security policy templates for immediate validation

Conclusion

Natroy Compliance turns configuration audits and security reviews into real-time, actionable processes. It helps organizations enforce standards, reduce risk exposure, and simplify audit response all while integrating with the automation and service management layers of the Natroy ecosystem.

Call to Action

Start with Natroy Compliance.

✉ info@natroy.io

🌐 www.natroy.io