NATROY

CVE Management: Intelligent Platform-Powered Vulnerability Resolution

Traditional CVE Management Falls Short

Most vulnerability solutions create overwhelming noise instead of actionable intelligence.

85%

False Positives

Traditional scanners flag vulnerabilities that don't actually apply to your specific device configurations.

Multiple

Disconnected Tools

Vulnerability scanning, asset discovery, change management all requiring complex integrations.

5000+

Alert Fatigue

Managing thousands of CVE alerts across enterprise infrastructure becomes overwhelming and ineffective.

What Makes Natroy CVE Management Unique

We don't just find vulnerabilities we determine if they actually matter and automatically fix them.

AI-Powered Context Analysis

Our AI analyzes each CVE against your actual device configuration, running services, and operational context to determine real applicability, not just version matching.

Intelligent Device Groupings

Process thousands of devices efficiently by grouping similar configurations and applying AI patterns once per group, not per device.

Lightweight Privacy-Preserving Validation

Execute targeted validation commands on devices without exposing sensitive configuration data only specific checks needed for each CVE.

info@natroy.io

Three-Path Smart Remediation

Automatically categorize vulnerabilities as Not Applicable, Configuration fixable, or Software Update required with full audit trail and evidence.

Enterprise-Scale UI Optimization

Purpose built interface for managing thousands of vulnerabilities with virtual scrolling, smart grouping, real-time filtering, and bulk operations.

Seamless NCI Integration

Works with your existing Non-Compliance Item (NCI) workflow no separate systems, no process changes, leverages current infrastructure.

The Power of Platform Integration

Natroy CVE Management leverages the entire platform ecosystem no external integrations needed.

Asset Discovery

Real-time device inventory and configuration awareness

Continuous Monitoring

Real-time security posture tracking and alerting.

Configuration Management

Direct device access for validation and remediation.

Compliance Engine

Automatic compliance validation and reporting.

Change Automation

Automated deployment of security fixes and configurations.

info@natroy.io

How Our AI Changes Everything

- Traditional scanners: "This version has a CVE" .
- Natroy: "This CVE actually affects your specific setup and here's how to fix it".

1

CVE Intelligence Analysis

AI analyzes CVE details, attack vectors, and prerequisites to understand what conditions make a device actually vulnerable.

2

Smart Pattern Generation

Generate device type specific validation commands and patterns one AI call serves thousands of similar devices.

3

Contextual Validation

Execute lightweight checks on devices to confirm if vulnerable conditions actually exist in your environment.

4

Intelligent Classification

Automatically categorize each vulnerability with confidence scores, detailed evidence, and recommended remediation paths.

Complete End-to-End Automated Workflow

From detection to resolution all within one unified platform.

1

Intelligent Detection

AI analyzes CVEs against actual device configurations and operational context, not just version numbers.

Powered by: Asset Discovery + AI Analysis Engine

2

Contextual Validation

Execute targeted commands to confirm vulnerability applicability without exposing configurations.

Powered by: Configuration Management Module

3

Automated Remediation

Generate and deploy configuration changes or schedule updates automatically with approval workflows.

Powered by: Change Automation Engine

4

Compliance Validation

Verify fixes are applied correctly and maintain ongoing compliance monitoring.

Powered by: Compliance Engine + Continuous Monitoring

info@natroy.io

Built for Enterprise Scale

Handle the complexity of large network infrastructures with intelligent automation.

5000+
Devices Analyzed Simultaneously

99%
Reduction in AI API Calls

30min
Full Analysis Completion

100%
Audit Trail Coverage

Traditional Approach vs. Natroy Platform

Why building integrations is yesterday's approach.

Traditional CVE Tools

- ⊗ Standalone vulnerability scanner.
- ⊗ Manual asset inventory integration.
- ⊗ Custom API connections to CMDB.
- ⊗ Separate change management process.
- ⊗ Manual compliance validation.
- ⊗ Weeks to implement integrations.
- ⊗ Data sync issues and conflicts.
- ⊗ Limited remediation capabilities.
- ⊗ High false positive rates.
- ⊗ No contextual analysis.

Natroy Platform

- ✓ Platform-native CVE management.
- ✓ Built-in real-time asset discovery.
- ✓ Native configuration management.
- ✓ Integrated change automation.
- ✓ Automatic compliance validation.
- ✓ Instant deployment no integrations.
- ✓ Single source of truth.
- ✓ Complete automated remediation.
- ✓ AI-powered context analysis.
- ✓ Enterprise-scale UI optimization.

info@natroy.io

Measurable Business Impact

Transform your vulnerability management from reactive noise to proactive intelligence.

60%

Reduction in False Positives

Focus on vulnerabilities that actually matter to your environment with AI-powered context analysis

40%

Time Savings

Eliminate manual verification of non-applicable vulnerabilities through automated validation

90%

Faster Remediation

Clear action paths and automated deployment mean faster resolution of real threats

info@natroy.io