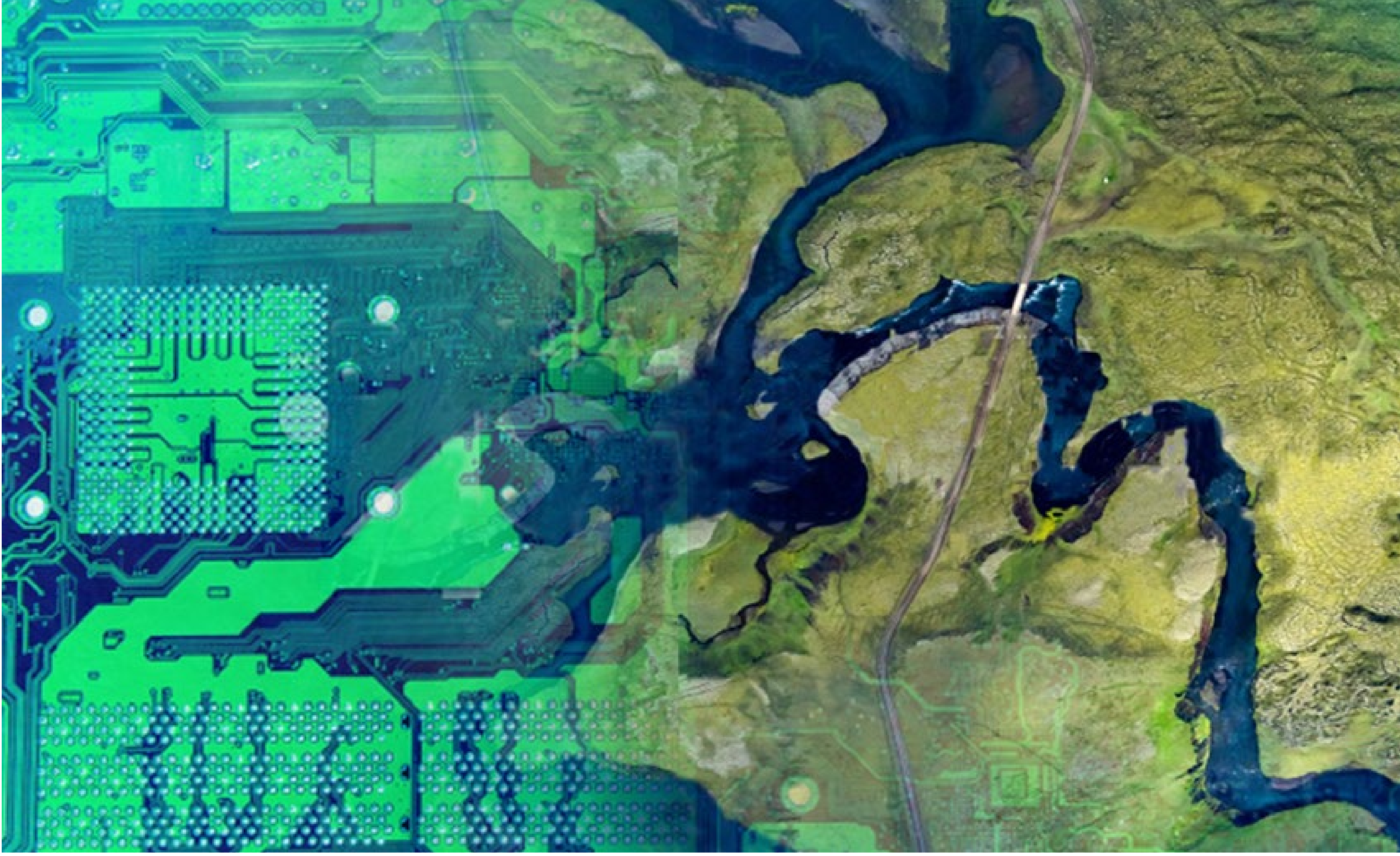


A Simplified and Sustainable Approach to NERC CIP Compliance with Cyberwiz-Pro

CYBERWIZ-PRO™

NERC CIP
Compliance Solutions from WizNucleus

1 EXECUTIVE SUMMARY

1.1 THE CHALLENGE

Electric utilities that contribute to the bulk electric system (BES) must comply with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards. Electric utilities with high and medium impact cyber assets have spent considerable time and resource to become compliant with NERC CIP.

Companies have learned that, in order to maintain and sustain a cost-effective and efficient program, they need to enhance their approach in a number of ways such as:

- Maintaining the configuration baseline by automatically discovering assets and detecting configuration changes
- Automating a tight change control process with approvals, escalations, impact analysis, test plans, and change verification
- Performing security control tests for significant changes, analyzing the results, and associating the test results with the appropriate CIP Cyber Assets
- Integrating security products such as patch management, event logging, access management into the compliance process
- Tracking reviews of authorizations to individuals who have been granted either unescorted physical access or logical access to CIP Cyber Assets
- Documenting the review and investigation of security log events and alerts
- Ensuring that all compliance evidence can be associated with the appropriate CIP Cyber Assets

Companies realize that a sustainable, cost-effective program takes more than spreadsheets and SharePoint. In addition, it's becoming evident that customizing IT tools, such as GRC, is a never-ending, costly and difficult task.

This paper describes how Cyberwiz-Pro helps companies create a more efficient and sustainable program while saving more than 50% on the human resource cost of that program and implementing it more quickly.

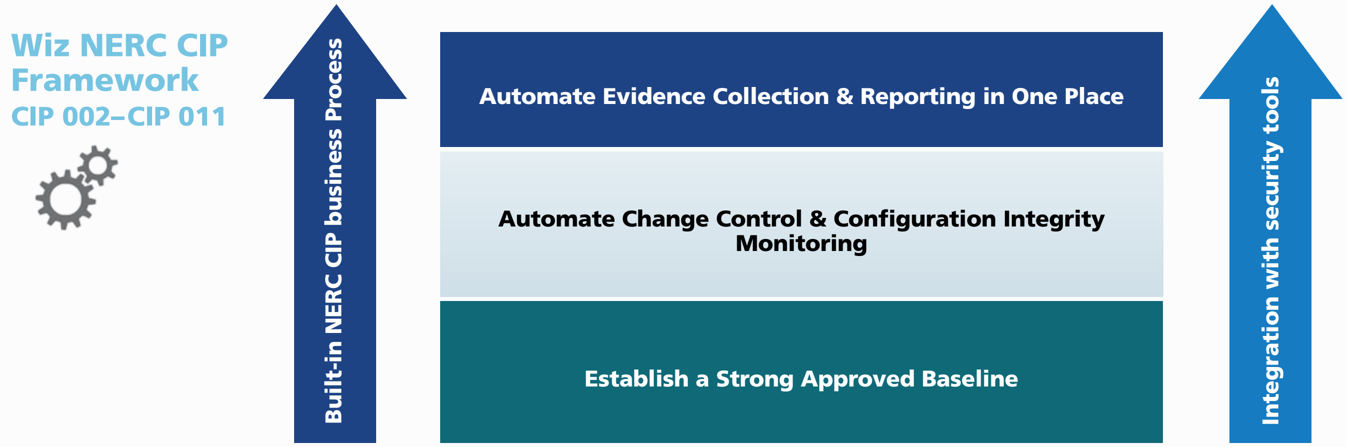
10 KEY ADVANTAGES OF THE WIZ FRAMEWORK

1. **A business process built into the tool that maps specifically to NERC CIP**
2. **Centralize existing asset descriptions by importing from spreadsheets, databases, other asset management tools**
3. **Automatically discovering ports, services, applications, patches and users**
4. **Wizard-driven classification techniques**
5. **Providing a closed-loop workflow for change management allowing for click-through assessments of the change for items such as approvals, escalations, impact analysis, test plans, and automatically keeping the baseline up to date**
6. **Configuration Integrity Monitoring ensuring changes are approved**
7. **Centralized vulnerability analysis expedites the assessment process using grouping techniques**
8. **Automated evidence gathering, reports and dashboards specific to NERC CIP come pre-defined and standard**
9. **Pre-defined integration with other security tools such as log management and patch management**
10. **Creating an overall better and well managed compliance program**

1.2 THE SOLUTION

Cyberwiz-Pro (CWP) is built specifically to manage NERC CIP compliance (CIP 002-CIP 011). CWP has a built in NERC CIP business process that guides and aides the user through each CIP standard with an easy-to-use and customizable workflow. CWP includes strong configuration baseline creation, change management workflows to keep the baseline approved, and evidence gathering and reporting capabilities with the ability to look at the overall picture of the CIP program as well as drill down into the details for analysis, evaluation and evidence gathering.

The following diagram depicts the Wiz Framework for NERC CIP.


Wiz NERC CIP Framework
CIP 002–CIP 011
Built-in NERC CIP business Process
Automate Evidence Collection & Reporting in One Place
Automate Change Control & Configuration Integrity Monitoring
Establish a Strong Approved Baseline
Integration with security tools

The foundation of the framework is built on a strong approved baseline that is the basis of all CIP activities.

The baseline is built by:

- importing existing asset data from a database or spreadsheet,
- **automatically discovering** ports, services, applications, patches, and users through a **powerful CWP agent**,
- integration with other products such as Tripwire,
- using a wizard to **classify** assets,
- providing documented approval of the baseline

All of these features are designed to save time, reduce human errors, and make the compliance efforts repeatable and efficient. Built on a relational database, CWP provides many capabilities to help manage the asset data and approved baseline.

An easy-to-use business process workflow engine provides the basis for a NERC CIP change and configuration management process. A task-driven interface guides the user through the change process steps such as change creation, approvals, escalations, impact analysis, test plan, implementation plan, and change verification. The configuration is monitored for changes to ensure proper approvals exist. The baseline is updated automatically.

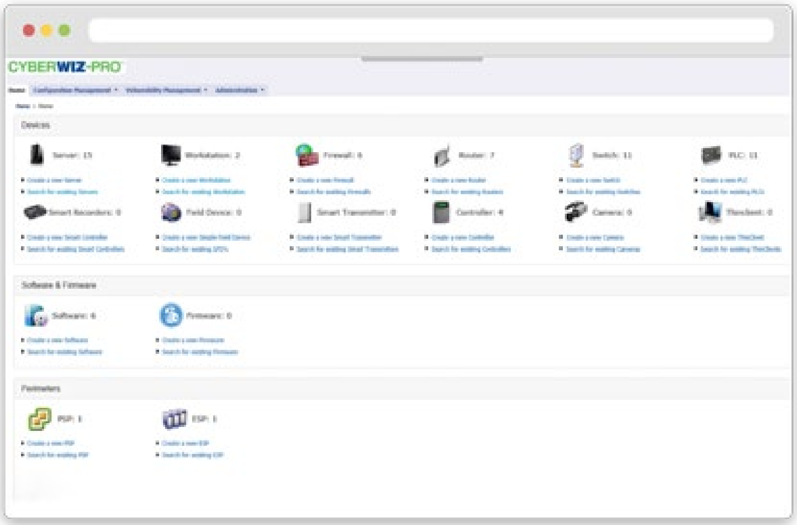
CWP comes with very powerful high-level executive reports as well as detailed reports. CWP collects a wealth of information about the assets and users. This information comes to life with CWP reporting.

2. ESTABLISH A STRONG BASELINE

2.1 OVERVIEW

All the baseline assets and attributes are housed in an easy-to-use, searchable relationship database. All the assets are available at-a-glance with the ability to drill down to see things such as ports, services, and patches.

CWP maintains a complete audit trail of all changes to the baseline, including approvals and test plans, making it easy to pull an audit report at any time. This task is virtually impossible to maintain on any sustainable, repeatable basis without a product like CWP.



2.2 GETTING STARTED—IMPORT YOUR EXISTING ASSETS

Today, many customers are struggling with their approach to maintaining an approved baseline by using spreadsheets especially if there are multiple sites, making it difficult to have one centralized database of record for assets. Other customers may be using a home-grown database or may have acquired an IT asset management product from another vendor.

CWP can accommodate the import of assets from each of these various methods making it easy to get started with NERC CIP compliance. The CWP agent automatically discovers ports, services, applications, patches and users. CWP can also capture asset data directly from other products such as Tripwire..

2.3 ADD AN ASSET

Creating the configuration baseline with all the appropriate asset details can be very laborious and prone to human error. CWP can automatically discover assets and then pull the asset details from the device.

Customers can build out the detailed inventory in a fraction of the time, with fewer errors using CWP.

2.4 CLASSIFY THE ASSETS

CWP improves productivity by providing a built-in classification wizard that allows customers to navigate through the classification process. The wizard comes with many example questions and allows for you to add or change questions based on your classification process. If you're working with a consultant, the consultant's classification methodology can be documented here. The classification details are kept for historical auditing.

3. AUTOMATE CHANGE CONTROL AND MAINTAIN CONFIGURATION INTEGRITY

Once the baseline is established, it's important to keep it current and approved, allowing for planned changes as well as monitoring for unplanned or unapproved changes.

CWP comes with an enterprise grade business process workflow engine, designed specifically for NERC CIP. It comes pre-configured with the following process steps:

- Create change request
- Approvals based on customer process (at each step; multiple approval levels, escalations)
- Operations engineering analysis
  - Impact analysis
  - Emergency analysis
  - NERC analysis
- Creation of the test plan
- Ongoing monitoring for configuration changes

Users (reviewers, implementers, approvers) in the work flow have role-based inboxes that are set up for their personal work queue. Users can review the change detail along with the devices that are impacted as well as the CIP requirements that accompany that change. Device details and CIP details are available directly on the screen for reference.

Assessment information can be added for by each reviewer, making the information available to all the users at each step of the process, as well as being logged for evidence.

CWP monitors things such as ports, services, patches, and user accounts for any change to the baseline. For example, if there is a change to a port, and alert is sent to the person responsible for evaluating that change. If it was an unapproved change a user might check to see if it was an emergency change and deal with it accordingly (e.g., approve). If it was an unapproved change then the user has the ability to restore to the original baseline.

4. EXPEDITE VULNERABILITY ASSESSMENTS

Performing vulnerability assessments on all the BES Cyber assets can be onerous. The CIP vulnerability assessment is not your typical assessment. CIP 010 mandates that High and Medium Impact BES Cyber Systems are periodically assessed by either an active or paper based vulnerability assessment to ensure the integrity of the recorded baseline configuration. This is in large a paper exercise that quickly becomes unmanageable without CWP.

4.1 MANAGE AND ORGANIZE THE LARGE AMOUNT OF ASSESSMENT DATA

CWP provides a way to organize assessment data to enhance productivity and efficiency by asset and class of asset. Observations, decisions, corrective actions can be recorded in CWP, which can be made available in reports and dashboards to support audits.

4.2 BUILT IN VULNERABILITY LIBRARY

CWP has the vulnerability library built into the product. The library is modified regularly to reflect changes to the standards and the type of resource.

4.3 ABILITY TO GROUP ASSETS BY CLASS WITH SIMILAR VULNERABILITIES (E.G., WINDOWS SERVERS)

For example, assets with similar assessment characteristics can be grouped together in the assessment evidence.

4.4 REPEATABLE (ASSESSMENTS MUST BE PERFORMED EVERY YEAR) AND REDUCE HUMAN ERRORS

Vulnerability assessments have to be repeated every 15 months. Customers can take advantage of previous assessments since all the assessment data is in CWP.

5. ALL THE EVIDENCE IN ONE PLACE— ALWAYS AUDIT READY

CIP 002— Identify and categorize BES Cyber Assets as described in step 1

CIP 003—security controls—tracks changes to policies

CIP 004—maintain a personnel training schedule and centralized repository for all training documentation

CIP 005—Electronic Security Perimeter—generates network diagrams

CIP 006— Physical Security of BES Cyber Assets—tracks policy and changes to policy. Maintains access lists

CIP 007—As described in step 2 and 3, automates ports, services and user account change management and monitoring; integrates change control with patch management systems to maintain integrity of the CIP program; maintains and tracks procedural controls

CIP 008—Incident Reporting and Response Planning—CWP provides a central repository to store documents or link to those documents for easy one touch audit

CIP 009—Recover Plans—CWP provides a central repository to store documents or link to those documents

CIP 010—As described in step 3, CWP monitors changes to the configuration and alerts on those changes per the built-in workflow engine. As described in step 4, vulnerability assessments are expedited using a full built-in library of controls as well as grouping assets to minimize assessment descriptions.

CIP 011—Information Protection—centralize documents, SIEM integration?

6. AUTOMATE REPORTING AND TRACKING

Reports are available for various levels of the organization. Executives can see the overall compliance picture—what's been done and what tasks are yet to be completed. Managers an see what tasks are completed, upcoming, in progress, or what has fallen behind schedule. In addition, CWP gives the user that ability to create ad hoc reports. Ad hoc reporting is a powerful tool to help organize data based on the CWP relational database and wealth of information.

SUMMARY

With CWP, companies can create a strong, repeatable CIP program, more efficiently while reducing cost. CWP can pay for itself within the first six months of the program by:

- Simplifying asset inventory and classification
- Creating a solid configuration and change management process with a solid, predictable workflow
- Monitoring changes to ensure policies are enforced
- Quickly creating and gathering evidence
- Managing compliance data with a relational database for CIP 002-011
- Expediting vulnerability assessments by managing assessment data and grouping assets
- Generating high-level executive reports, detailed reports, and audit reports

Create a sustainable NERC CIP program with CWP that is always audit-ready.

Contact us

WizNucleus, Inc.
200 Park Ave, Suite 1700
New York, NY 10017
(866) 949-4431
www.wiznucleus.com