ConsoleWorks
Cybersecurity Operations Platform

Automated Patch Analysis

PEOPLE • DEVICES • ACCESS

- Privileged Interactive Access
- Asset, Patch & Configuration Monitoring
- Logging & Situational Awareness
- Endpoint Password Management

NERC CIP-007-6 / R2 requires a patch management process for tracking, evaluating, and installing cybersecurity patches for applicable Cyber Assets – including device drivers. Many utilities see this is a grueling task, requiring many, many man-hours to meet the "every 35-day analysis" required by NERC CIP.

Utilities are in various stages of implementation of an effective solution with most relying on a manual update of a database, or spreadsheet, that contains the latest patch versions entered for each asset. The asset information, traditionally, has been manually gathered and manually entered since these approaches are disconnected from the assets. These and other manual approaches not only result in inconsistencies and errors, but are enormously labor intensive.

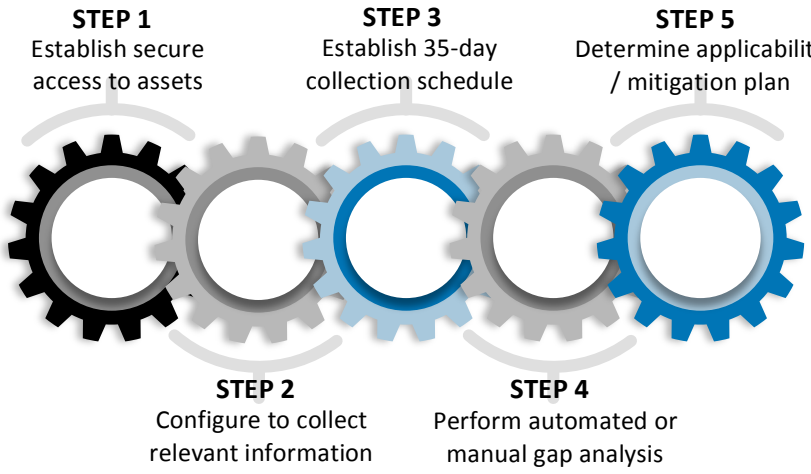
While there are effective Patch Management solutions available for IT devices, OT devices pose some particular challenges that require knowledge, experience and understanding of:

- various communications protocols (IP, Powershell, HTTP, Serial, Modbus, DNP3 and others)
- vendor authorized method of collecting patch information from the assets (command line, web interface, manual)
- information required to collect from the assets
- the relationship between software and firmware
- when HMIs are not treated as typical Windows® devices – vendor source is not Microsoft®

The ConsoleWorks Automated Patch Analysis solution greatly simplifies the process of gathering the information required for patching IT and OT devices – beyond the HMI, all the way to the last leaf.

For meeting NERC CIP compliance, ConsoleWorks is configured via a schedule to perform the patch analysis every 35 days, keeping a log, for audit purposes, of when the analysis was run. Once the current patch state is gathered by ConsoleWorks, ConsoleWorks can integrate with industry or custom solutions to assist in automating the patch gap analysis. In these cases, ConsoleWorks sanitizes, anonymizes, and encrypts the data before initiating the secure transfer of the collected device information.

After the initial collection is sent, ConsoleWorks can be configured to continually monitor for the patch gap analysis results. When available, ConsoleWorks automatically downloads and processes the results, using ConsoleWorks Events as an indication to the user when patches are available. Event Severities further indicate whether an available patch is a security patch.

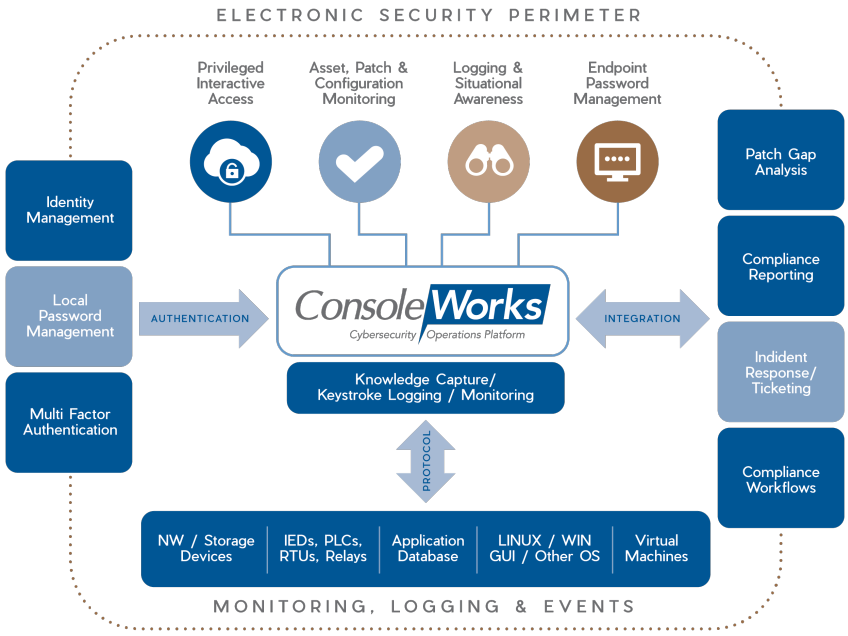


Finally, ConsoleWorks produces dashboard report views to organize and communicate the current patch state. ConsoleWorks presents a summary report containing information on patch gaps that may exist for each asset, including links to any available patch for downloading directly from the vendor site.

At this point, a utility will evaluate the available security patch for applicability and make the decision to install the patch or initiate a mitigation plan.

ConsoleWorks' integration with workflow management solutions enables utilities to further automate the patching and mitigation processes as required by NERC.

The patch analysis features will be available in ConsoleWorks in Q1, 2018, and are part of a larger cybersecurity and operations platform solution addressing many of the NERC CIP V6 requirements for Secure Remote Access, Asset and Configuration Monitoring, Endpoint Password Management, Logging and Situational Awareness and Supply Chain - CIP-005, CIP-007, CIP-010, and CIP-013.



sales@tditechnologies.com | 800-695-1258 | tditechnologies.com