VENDOR-AGNOSTIC NERC CIP COMPLIANCE COVERAGE

CASE STUDY

Leading power company used Verve Industrial Protection to achieve target NERC CIP coverage across multiple OEM systems

Cyber security in an industrial setting can be complicated, requires multiple tool sets from different vendors and is difficult to maintain. Verve developed a platform-based approach for support across multiple vendors and coverage to all assets. It is significantly faster, more accurate and requires less resources than current, silo'd offerings.

This document outlines a brief introduction to our solution and explains how a regulated entity chose to replace its vendor-specific tools with our more inclusive approach.

THE CHALLENGE

A large power generation company rolled out the Verve Security Center to their medium-impact NERC regulated locations. In some cases, they already had multiple security tools in place, provided by the OEMs, with no integration. In other cases, they had to begin from scratch. But like many utilities companies, they had a short window in which to achieve compliance. In one example, they only had a few weeks from the time a plant was acquired until it needed to be compliant with NERC CIP v5.

The client aspired to have a single platform that spanned all vendors across its globally-dispersed plants. It needed to work well with Emerson, GE, ABB, Rockwell, Schweitzer, and a dozen other vendors. Further, they wanted an integrated console to integrate data from all NERC CIP requirements into one dashboard for centralized compliance reporting. Lastly, they wanted a solution to work through diodes or other implemented network architectures to reduce access into their sites.

THE SOLUTION

The client decided to standardize on a common, vendor-agnostics security platform, namely the Verve Security Center (VSC). Built to span individual security tools across multiple OEM vendors and report out and up through air gaps or data diodes, the VSC enabled the client to meet its objectives of simplicity and efficiency.

TRADITIONAL ICS SECURITY

The Verve Security Center is a departure from most security tools available on the market today. Most security offerings are silo'd or vertical tools that specialize in a particular security function or practice. In industrial controls environments, OEMs may each have their own set of tools, leaving customers to manage multiple anti-virus, SIEM backup or inventory systems.

Once an entity follows this practice to procure and configure multiple tools to address multiple risks, they end up with a collection of silo'd, possibly under-used or ineffective tools that bear no references to one another - and may require significant manual input to derive value.

The multitude of tools requires specific skill sets and experience in each practice, greatly increasing the training and awareness required for the individuals accessing this information.

We often find industrial sites do not have the staff or budget to train and retain the various security-specific skill sets. Disconnected cyber security tools makes collecting information time-consuming, manual and prone to error.

Verve Security Center was created as a direct response to solve these three challenges:

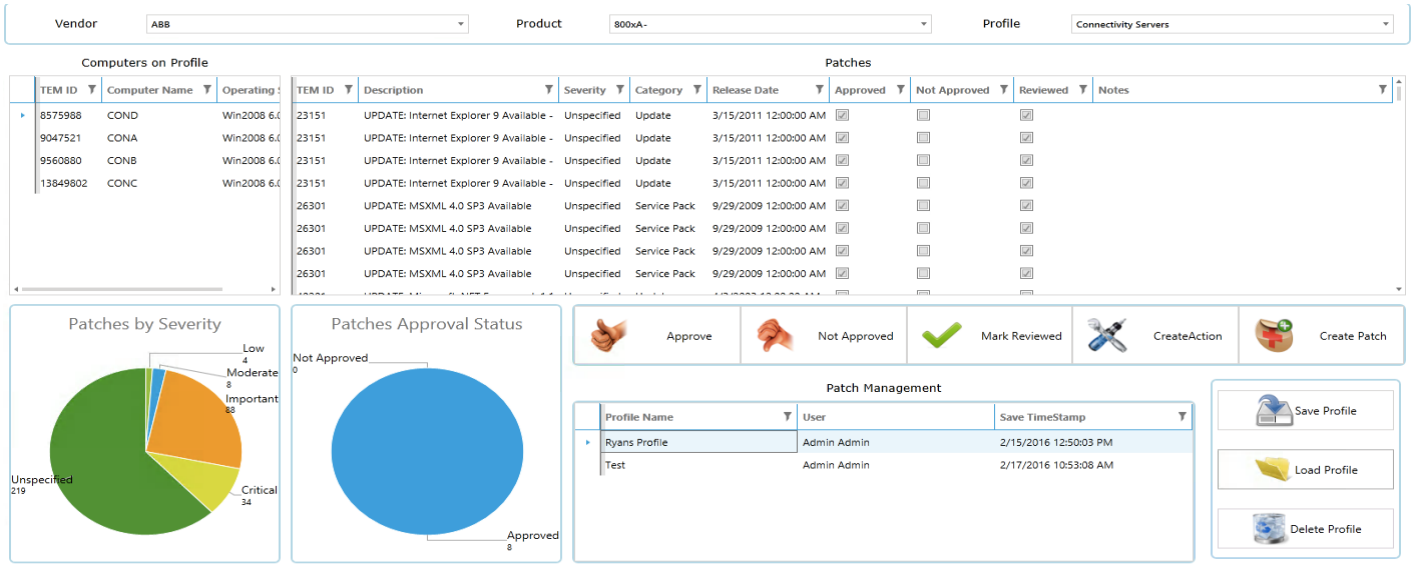
- Complexity of NERC CIP compliance/security in an OT environment
- Capture value in existing IT tools and other investments
- Improve efficiency and accuracy of security support services (internal, external or targeted)

VERVE SECURITY CENTER

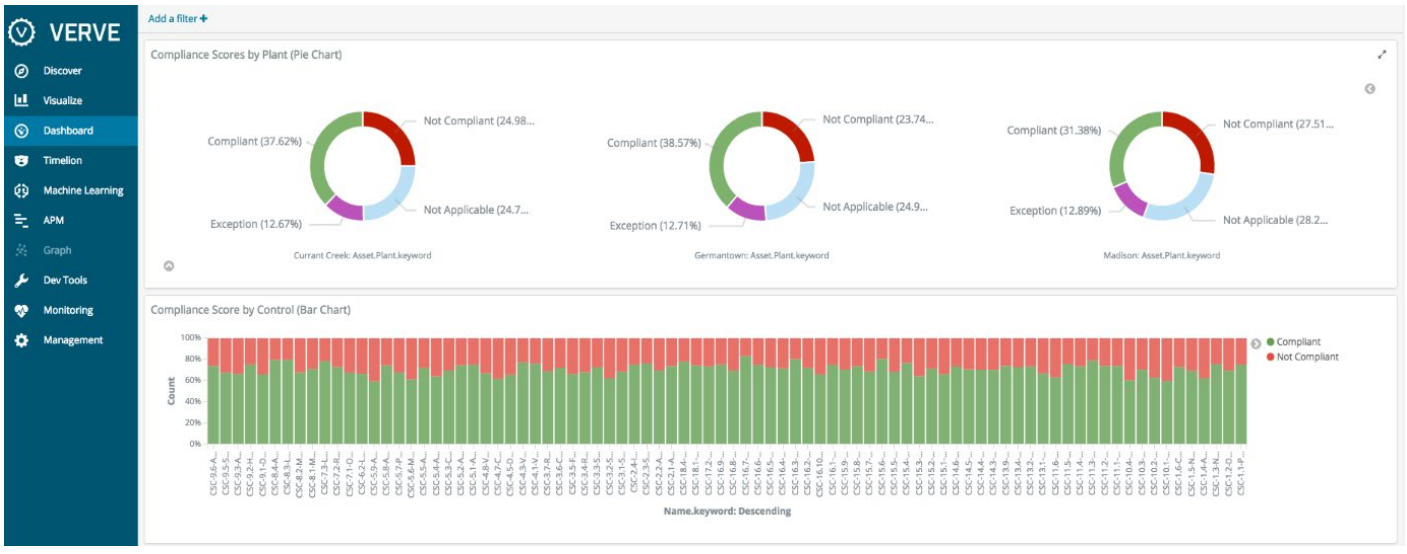
VSC is a purpose-built solution to the complexities of OT/ICS cyber security compliance. The product comes from the 25-year legacy of Verve Industrial Protection as a control system integrator designing and implementing ICS controls across the power industry and other process industries.

Over a decade ago, our team started building a solution for the needs of the power industry as NERC CIP was designed and implemented. Our experience in plants led us to understand the challenges of multi-vendor environments, and our knowledge of cyber security led us to realize the challenges of silo'd toolkits. Our experience as operators gives us unique perspective into the challenges of the labor shortage needed to achieve compliance reporting. Overall, our experience culminated in a vendor-agnostic ICS cyber security platform - the Verve Security Center.

Verve provides a comprehensive suite of security components to meet all technical requirements of NERC CIP v5/6. This includes: asset inventory, patching, whitelisting, anti-virus, backups, SIEM, vulnerability assessment, configuration management, etc. The platform brings all data into a single interface for streamlined reporting. Because of it's architecture, users take actions to ensure compliance actions are completed on a timely basis - such as patching every 35 days.



This information is centralized across sites for easy visibility to compliance on all metrics across all sites.



THE PROJECT

The first step was installing our agent-agentless approach across all vendor systems. Verve's architecture leverages a lightweight agent that enables us to monitor and develop asset information, as well as address compliance tasks such as vulnerability assessment, patching, configuration management, etc. Our agentless approach extends visibility and management to the embedded devices such as networking equipment, PLCs, relays, etc.

The unique architecture delivered several of the key components of the NERC CIP requirements: comprehensive asset inventory, vulnerability assessment, patch management, ports and services, configuration review, etc. We integrated SIEM functionality through log management to identify key compliance items such as failed logins. We then integrated third-party tools the client had already purchased through its OEMs, such as backups from Acronis and anti-virus (multiple vendors depending on OEM requirements). We deployed application whitelisting and put it into lock-down mode to ensure no unapproved software could run in the system. Overall, Verve provided comprehensive coverage for NERC CIP v5.

The next step leveraged the strength of the Verve Security Center along with Verve Industrial Protection (VIP) Services to ensure the client achieved compliance. We pulled baseline information, remove unnecessary ports and services, confirm backups were up-to-date, etc. Within three weeks at one plant, we accomplished these steps without disruption while the plant remained online.

The final phase included the application of the tools and data capture of their effect. We used our central reporting platform to assist in the profiling of all assets before and after the application of security controls such as vulnerability scans, baselines and backup/restoration points. Then patches were deployed, whitelisting profiles were configured, and we re-ran summary reports around patch levels and in-use/acceptable ports and services in use.

> “Verve was awarded this work after a bidding process that also included Emerson Ovation, ABB and Honeywell because of their **platform-agnostic solution.**”

> “If we bought separate cyber solutions that each OEM offers, it would be impossible to manage all the different tools and implementation strategies.”

THE IMPACT

The integrated capabilities of Verve - across OEM vendors' equipment and necessary components of NERC CIP allowed our power client to reduce their total cost of ownership of their ICS compliance. They simplified the complexity of multiple security tools across different OEM vendors and created a consistent view into common security practices from a central regulatory and support perspective.

The Verve Security Center provides a programmatic response to the emerging needs of ICS cyber security trends. The comprehensive platform reduces complexity in managing security and compliance programs by tying together otherwise disparate data sources into a single platform to improve the speed and accuracy of data collection and review.

Our unique approach captures value from existing security investments. By incorporating multiple tools into a single reporting and alerting console, action required by otherwise silo'd systems is captured and tracked.

This supports the instant analysis of emerging threats of programmatic lapses in our reporting. The data can also be ported to corporate support (SOC) or subject matter experts (managed services or other corporate departments) to reduce the demand on operational teams to maintain scarce and costly skill sets for compliance.

This power client improved and enhanced their overall cyber security program by simplifying their technical footprint and extending a familiar platform and tool set to additional physical locations. Verve continues to work with this client on additional locations to pull site-specific data into an enterprise-wide roll up of their efforts.

> “Once Verve detailed their configuration plan, **I had full confidence** it wouldn't cause any control system issues. We are even connected to the proprietary DeltaV switches.”

> “It's not that other solutions won't work, but we want **one set of tools** for every plant and every system.”