Case Study

VENDOR-AGNOSTIC NERC CIP COMPLIANCE COVERAGE

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

Cybersecurity in an industrial setting can be complicated, requires multiple tool sets from different vendors and is difficult to maintain. Verve has developed a platform-based approach that allows for support across multiple vendors, provides coverage to all assets and is significantly faster, more accurate and requires less resources than current, siloed offerings. The balance of 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

VERVE INDUSTRIAL PROTECTION

Client Profile & Challenge

The client in question is a large power generation company that 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 were beginning from scratch with a clean slate. But, like many utilities they had a very short window in which to achieve compliance. In one case, they only had a few weeks from the time a plant was acquired until it had to be compliant with NERC CIP v5.

The client's aspiration was to have a single platform that spanned all vendors in its plants across the country. It needed to work with Emerson, GE, ABB, Rockwell, Schweitzer, and another dozen vendors. Further, they wanted an integrated console to bring data from all of the underlying NERC CIP requirements into one dashboard and reporting function for compliance reporting. Finally, it had to work through diodes or other network architectures that they had implemented to reduce access into their sites.

The Solution

Our client decided that the best thing to do was to standardize on a common, vendor-agnostics security platform, namely the Verve Security Center. Built to span individual security tools across multiple OEM vendors and to 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 (VSC) is a departure from most security tools available on the market today. Most security offerings are what we call 'siloed' or vertical tools that specialize in a particular security function or practice. Furthermore, in industrial controls environments, OEMs may each have their own set of tools, leaving customers to manage multiple AV, 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 siloed, possibly under-used or ineffective tools that bear no reference to one another and require significant manual input to derive value. Moreover, this multitude of tools require specific skill sets and experience in each of the individual practices thereby greatly increasing the training and awareness required of the individuals accessing this information. And we often find that industrial sites simply do not have the staff or budget to train and retain a multitude of security specific skill sets. Finally, the fact that these tools are not tied

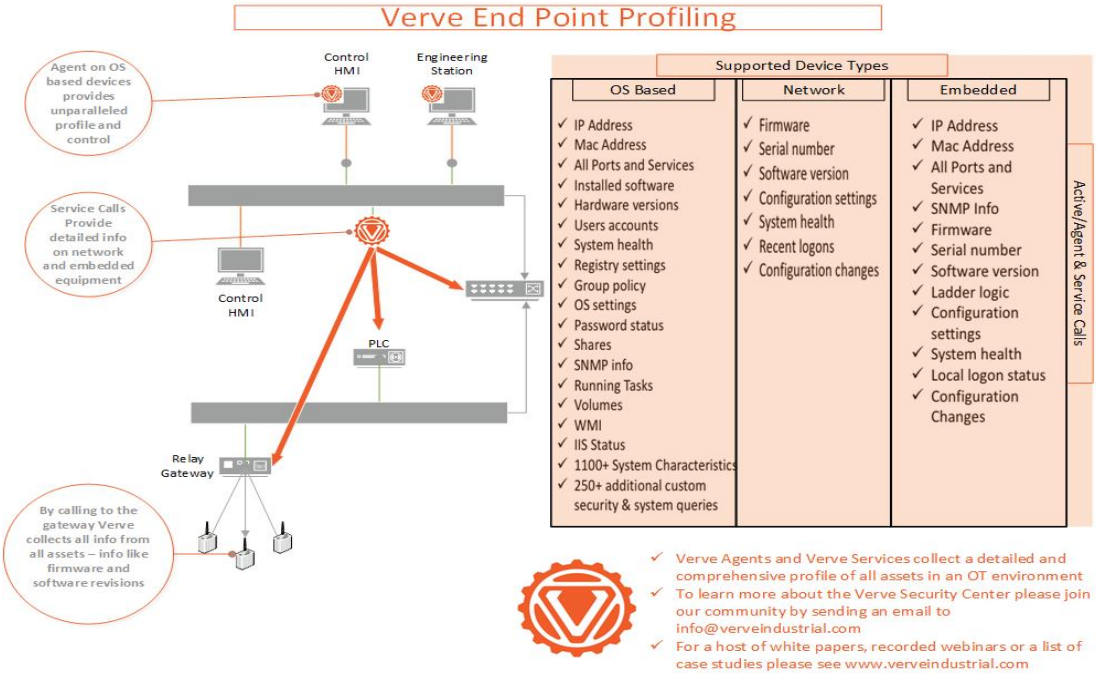
together means that collecting information from the various tools is time consuming, manual and prone to error.

This is the premise under which we created VSC. It is a direct response to solving the following 3 challenges:

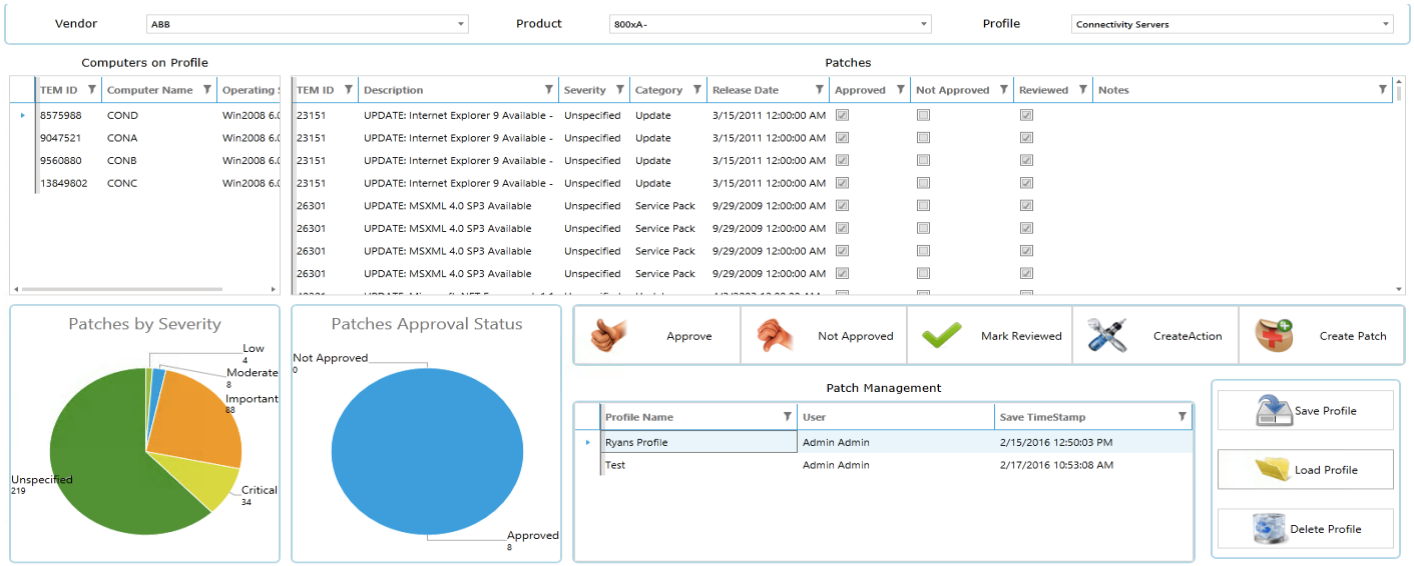
- Complexity of NERC CIP compliance/security in an OT environment
- Capture value in existing IT tools and investment
- Improve efficiency and accuracy of security support services (internal, external or targeted)

Verve Security Center

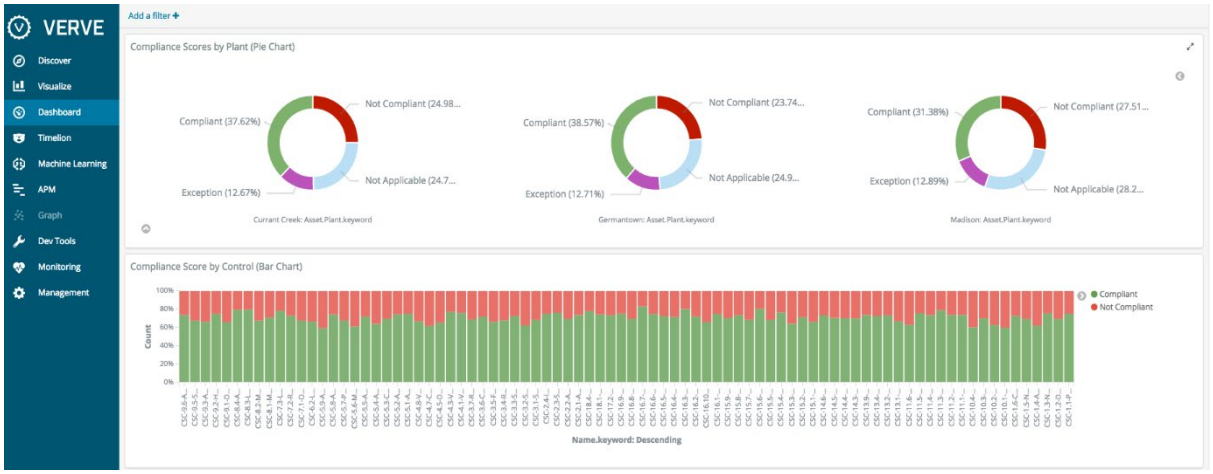
VSC is a purpose-built solution to the complexities of OT/ICS cyber security compliance. The product comes from the 25-year legacy of Verve Industrial Protection as a control systems integrator designing and implementing ICS controls across the power industry as well as many other process industries. Over a decade ago, our team began building a solution for the needs of the power industry as NERC CIP was being designed and implemented. Our experience in plants led us to realize the challenges of multi-vendor environments. Our knowledge of cyber security led us to realize the challenges of siloed toolkits. Our experience as operators led us to realize the challenges of the labor shortage to achieve compliance reporting. All of this experience culminated in the Verve Security Center – a vendor-agnostic ICS cyber security platform.



Verve provides a comprehensive suite of security components to meet all of the technical requirements of NERC CIP v5/6. This includes: asset inventory, patching, whitelisting, antivirus, backups, SIEM, vulnerability assessment, configuration management, etc. The platform brings all of that data into a single interface to allow for streamlined reporting. Further, because of its architecture, it allows the user to take action to ensure compliance actions are completed on a timely basis – such as patching every 35 days.



All of this information is then centralized across sites so that it provides easy visibility to compliance on all metrics across all sites.



VERVE INDUSTRIAL PROTECTION

The Project

The first stage of our effort was to install our agent-agentless approach across all vendor systems. Verve's architecture leverages a very lightweight agent that enables us not only to monitor and develop asset information, but also to address compliance tasks such as vulnerability assessment, patching, configuration management, etc. Our agentless approach extends that visibility and management to the embedded devices such as networking equipment, PLCs, relays, etc.

We used this unique architecture to deliver several of the key components of the NERC CIP requirements: comprehensive asset inventory, vulnerability assessment, patch management, ports & services/configuration review, etc. Further we integrated SIEM functionality through log management to identify key compliance items such as failed logins, etc. We then integrated third party tools that the client had already purchased through its OEMs such as backups from Acronis and AntiVirus (multiple vendors depending on OEM requirements). Further, 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 our Verve Industrial Protection (VIP) Services to ensure that the client achieved compliance. We helped pull baseline information, remove unnecessary ports and services, confirm backups were up to date, etc. In one plant, we had to accomplish all of these steps within 3 weeks while the plant was online without disruption.

The final phase of our efforts included the application of the tools and data capture of their effect. In essence 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 before we rolled out patches, configured whitelisting profiles and then re-ran summary reports around patch levels and in-use/acceptable ports and services in use. In other words, we used our central, vendor neutral security platform to run the security program for our client.

Impact

The integrated capability of Verve – both across OEM vendors' equipment as well as across all the necessary components of NERC CIP allowed our clients to reduce their total-cost-of-ownership of their ICS compliance because of simplifying the complex tasks required. Our

customers' comments to us are testament to our pride in our solution.

- ***"Verve was awarded this work after bidding process that also included Emerson Ovation ABB and Honeywell to offer a platform agnostic solution."***
- ***"If we would have bought all of the separate solutions for cyber that each of the above OEM vendors offer, it would be near impossible to manage all of the different tools and implementation strategies."***
- ***"Once Verve detailed their configuration and plan I had full confidence that we wouldn't cause any control system issues. We are even connected to the proprietary Emerson DetaV swtiches."***
- ***It's not that the other solutions won't work, we just want one set of tools for every plant and every system."***

Summary

Our client was looking for a way to simplify the presence and prevalence of multiple security tools across different OEM vendors. They were looking to creating a standard, consistent view into common security practices from a central regulatory and support perspective at head office. More importantly they wanted to provide full security program coverage over multiple OEM vendor platforms with consistency and accuracy.

The Verve Security Center is a collective, programmatic response to the emerging needs of ICS cyber security trends. Our comprehensive platform helps to reduce complexity in managing security and compliance programs by tying together otherwise disparate data sources into a single platform thereby significantly improving the speed and accuracy of data collection and review. Secondly our approach helps our clients to capture value from their existing security investment. By incorporating multiple tools into a single reporting and alerting console action that is required by otherwise siloed systems is captured and tracked.

Finally, by pulling all the data together we can support instant analysis of emerging threats or of programmatic lapses in our reporting. That data can also be ported out to corporate support (SOC) or to subject matter experts (managed services or other corporate departments) thereby reducing the demand on the operational team to maintain scarce and costly skill sets for compliance.

VERVE INDUSTRIAL PROTECTION

In this case we improved and enhanced our clients overall program by simplifying their technical footprint and extending a familiar platform and tool set to additional physical locations. We continue to work with this client on rolling our platform to many more locations while simultaneously pulling site specific data into an enterprise wide roll up of their efforts. To learn more please see us at verveindustrial.com or contact us at info@verveindustrial.com