VERVE
INDUSTRIAL PROTECTION

Technical White Paper

END-TO-END ICS PATCHING

Simplifying the complexity of patching Industrial Control Systems with integrated software and services – across all OEM devices

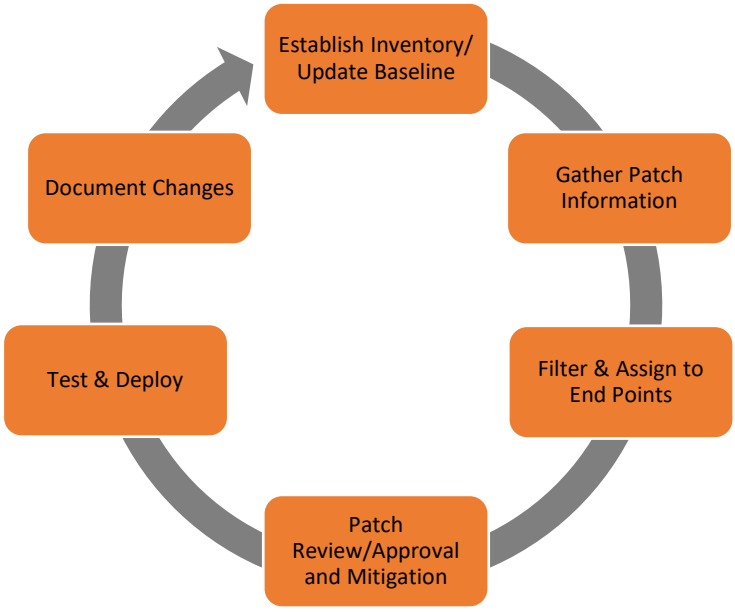
www.verveindustrial.com info@rkneal.com 1-270-442-9880

Patching – The Simplest Difficulty

Patching is often thought of as one of the most basic of all security practices. It appears, on the surface, to be such a straightforward process - simply apply updates to your systems. These updates are provided by the vendors that are intended to close any security or functional holes in your systems. This is so basic on paper that it is often overlooked or neglected by many security teams and system operators.

Patching, however, is not so straightforward after all. In fact, it is likely the single most time-consuming task that the North American Power Industry faces in adhering to regulatory expectations. This is due to a combination of factors, most notably:

- Lack of automatic inventory/monitoring of end systems
- Difficulty in monitoring patch releases for all systems/applications
- Time and expertise to review, approve, or mitigate patches in a workflow
- Testing and individually assigning patches to groups of end points
- Time to deploy on each device & confirm update working as appropriate
- Time to document changes & update baselines

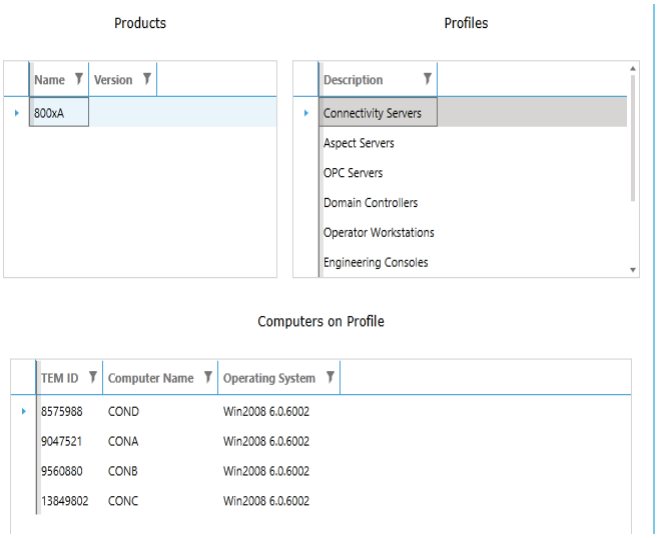


Because of these challenges, at Verve Industrial we have created an end-to-end patching process for our clients. Using a combination of our Verve Security Center (VSC) software and our Verve Engineering Services (both off site and on premise), we are able to both significantly

reduce the time & complexity and improve the quality and compliance-readiness by integrating each of the critical steps in a single-flow process. The following whitepaper outlines how our service offering aligns with the challenges listed above.

Inventory

The first problem for many organizations is understanding what they have plugged in, where it is and what software is deployed. Some organizations have managed to compile a reasonable list of assets either manually or through extension of existing corporate tools or agent based technologies. Almost all industrial operator networks, however, struggle to connect on a regular basis (let alone automatically) to the non-windows machines. In a typical operational network these proprietary systems make up close to 75% of all assets.



Our VSC provides visibility into all 100% of connected assets. Through a combination of our custom-tuned BigFix agent from IBM which covers the agent-based devices and our proprietary Foreign Device Interrogation Service (FDIS), we are able to inventory and monitor all assets in the OT network. Even more importantly, we can monitor all endpoints in even the most complex or challenging environments (like across low baud serial connections). We do so in a very low cost solution. Competitive solutions can cost up to 50X more to get the same data we do depending on the asset location.[1]

Gather Patch Information

The second challenge is the ability to monitor what patches are available. The core components of Windows, Linux, Unix, Office and other products like Adobe are straightforward (either from Microsoft or the OEM vendor-approved MS patches). Third party apps, however, usually require manual review of the vendor's website to look for new updates. Operators need to research patches to determine what, if any, security components are addressed. The sheer volume of these apps makes the task exponentially difficult. One of our clients is currently monitoring just under 300 third party apps that fall in this category just at one facility.

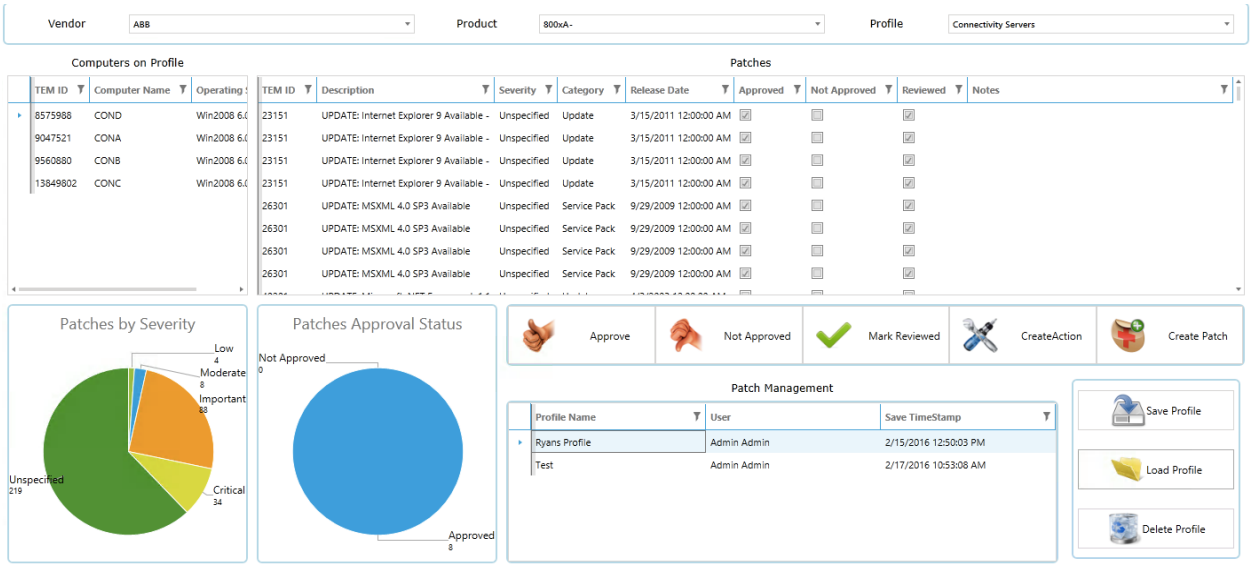
[1] 50X is a rough estimate generated by comparing our substation solution for monitoring relays for change management and log or SIEM collection functions when compared to our nearest competitor who requires a full deployment for their solution

Fortunately, Verve Engineering Services leverages the scale we have across clients to provide a much lower cost solution than any individual company can provide on their own. The client provides its list of third party apps to us. We will monitor the appropriate vendor communications and when a patch or update is published, we integrate that information into our Verve Security Center integrated patch solution.

Although this service is available to any of our clients regardless of whether or not they have VSC installed, integration adds significantly to the overall efficiency. When a client subscribes to our patch monitoring service AND is a VSC customer, we provide an electronic package that is preconfigured to import to the VSC deployment module. (See test & deploy below).

Filter and Assign to End Points

One of the most challenging elements of patching is to use the inventory to determine which assets should apply which updates – or filtering in other words. Verve has built the Verve Asset Manager (VAM) specifically to allow clients to automatically filter on the specific assets that are in scope for a particular patch. VSC can sort by any number of characteristics on the end device from type of OS to NERC CIP criticality ranking to any other specific characteristic of the target system. This filtering significantly speeds the analysis of what patch is required and on which systems.



Patch review/approval/mitigation

Many processes end there and leave the approval and action to another set of tools or processes. Verve Industrial brings the approvals and actions right into the same toolset. The VSC patching module allows for administrative functions such as marking patches as reviewed, approved or not approved. These actions are time stamped and the resulting specifics (ie time patch was entered to time until reviewed) are displayed on our patch aging dashboard.

Testing and Deployment

Testing is often a luxury that clients do not have time to conduct. We first use several techniques to ensure that the patch provided is the one that is approved and delivered from the vendor. VSC then allows the user to take the next step of programmatically deploying patches across OEM Windows/Unix/Linux devices right from the console. Importantly, the interface also allows you to schedule deployment on one or two assets initially to test that the update is working appropriately on less critical devices. It can then roll-back updates that are not working appropriately. Then the additional roll-out can be scheduled at any sequence.[2]. Additional controls such as rebooting (or not) the end device, displaying a message or retrying in case of failure are also configured in the console and are sent to the end device.

For those devices that cannot have a patch delivered, we offer professional, experienced staff who will come on site on a regular basis to deploy those patches to the agentless assets. Our engineers are exposed to all patches on all manner of equipment and as such have significant experience in the testing and deployment of patches. Moreover, they are well versed in operational knowledge as well so their respect for and understanding of control equipment is unparalleled. For many of our clients they manage the administrative review and approval of patches then leave it to us to support and manage the deployment of the approved packages thereby allowing company staff to focus on their operational tasks instead of repetitive compliance tasks.

Profiling and Documenting Systems

One of the more tedious regulatory tasks related to patching is the requirement to baseline systems before and after the application of a patch. Any changes to that baseline then need to be captured and entered into corporate change management workflows in order to capture the new configuration as well as to maintain compliance.

Fortunately for clients with VSC the baseline configuration before and after is automatic. Our agent based systems automatically flag any changes to target systems. More powerful, however, is the fact that our FDIS tool that inventories the 75% of agentless devices also has a parsing tool. This tool allows our clients to run a baseline after a patch and the parsing portion

[2] Automatic deployment of patches is recommended only under controlled circumstances and is only an option on agent base devices.

of the FDIS will capture any changes to that device. This extension of traditional change management function to agentless devices significantly reduces the manual effort of collecting and collating device baselines with respect to patching. Further, that same parsing tool can capture and feed both security logs and configuration changes to SIEM or change management tools for other compliance efforts.

Finally, our services team is also able to assist in the collection of baseline changes and to submit those changes to regulatory workflows and reporting tools within your organization.

Summary

What seems on the surface to be a straightforward function is actually quite difficult and time-consuming. Without automatic collection and monitoring tools the time and effort burden can be significant. Furthermore, manual tasks are much more prone to error thereby increasing time and effort on rework as well as potentially introducing risks to the systems themselves as well as to your regulatory standing.

Fortunately, Verve Industrial's end to end solution with its combination of on or off site services, powered by our innovative technology greatly increases the accuracy of our clients' efforts while simultaneously reducing the time and effort to complete these tasks. Our solution is flexible and scalable. Any or all of the products and services outlined in this paper are scalable to fit the client situation.

We welcome the opportunity to provide an initial diagnostic on the time and effort required of a client's current work process. We can then implement some or all of the controls suggested here and measure the time and accuracy of the program once our services have been tested. The resulting gain in time and accuracy will meet or exceed any corporate expectations for return on investment.