VIP Patching & Vulnerability Management

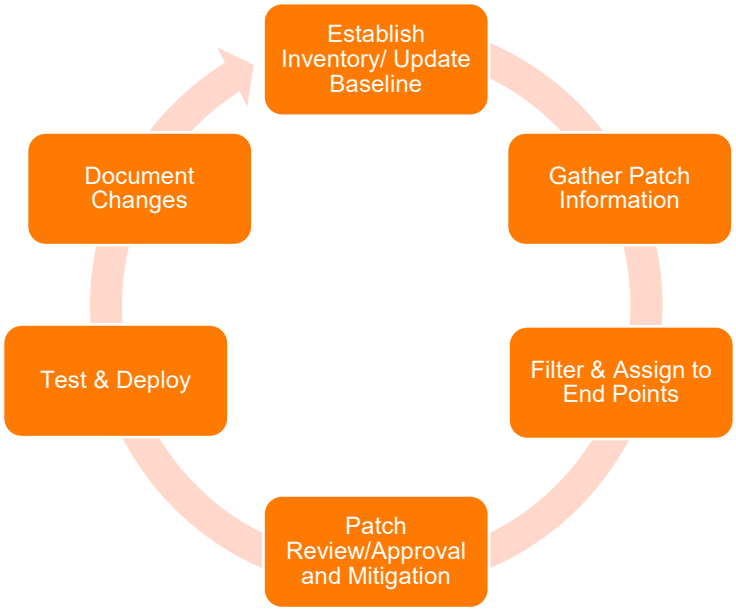
The Patch Challenge

Patching and vulnerability management in industrial control systems are full of challenges. From proprietary hardware and software to a lack of staff, inadequate or non-existent testing equipment and finally regulatory reporting and system maintenance many organizations are struggling to even sort out what is in scope, let alone manage patches.

Patching & vulnerability management is one of the most basic of all security practices. It appears as a key component on every major cybersecurity controls standard – NIST CSF, CIS/CSC20, ISA99, NERC CIP, etc. Unlike in IT where patching is a regular daily or weekly occurrence, however, in OT it is one of the single most difficult & time-consuming controls to meet. This is due to a combination of factors, most notably:

- Vulnerability & Patch Identification
  - Lack of dedicated OT vulnerability scanning tools
  - Lack of automatic inventory/monitoring of end systems
  - Difficulty in monitoring patch releases for all systems/applications
- Patch review
  - Time and expertise to review, approve, or mitigate patches in a workflow
  - Assigning relevant patches to groups of end points
- Patch deployment
  - In ability to take system offline to reboot
  - Time to test & deploy on each device & confirm update working as appropriate
  - Devices that cannot be patched without a hardware/system upgrade
- Compliance reporting
  - Time to document changes & update baselines
  - Integration of data across inventory, vulnerability, patch identification, approval, deployment, and re-baselining

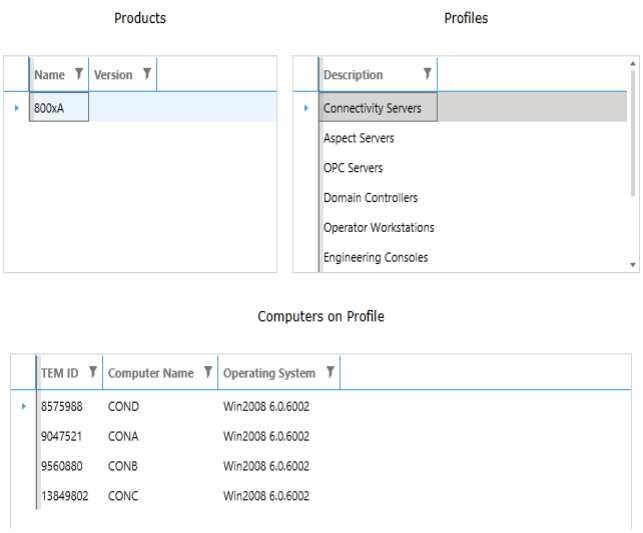
VERVE INDUSTRIAL PROTECTION



VIP: Technology + Talent Solution

Because of these challenges, at Verve Industrial Protection, we have created an end-to-end patching process for our clients. Using a combination of our Verve Security Center (VSC) software and our VIP Services (both off site and on premise), we can significantly reduce the time & complexity while improving the quality and compliance-readiness by integrating each of the critical steps in a single-flow process.

What is needed is a combination of leading OT vulnerability and patch management technology and expert talent services to augment the technology where it is not sufficient.



Inventory

To understand vulnerabilities and patch status, the first step is a robust asset inventory across all OS-based devices, networking equipment, and embedded devices. Verve Patch is integrated with Verve Asset Manager (VAM) which provides visibility into all of these assets. VAM is the only fit-for-purpose tool that can gather robust data on 100% of your assets…not just the ones that happen to communicate their firmware over the wire. Verve uses a combination of agent and agentless solutions to safely reach different types of assets, gaining the richest set of information available.

Gather Vulnerability & Patch Information

Because of Verve's rich asset (hardware, software, and firmware) inventory, Verve Security Center provides a robust vulnerability assessment without the need for risky vulnerability scanning from traditional IT tools. We compare our rich database of asset information against databases such as the National Vulnerability Database to identify potentially vulnerable versions of software and firmware. Importantly, these vulnerabilities are all tied back to a specific piece of software on a specific machine, so no longer is there a gap in information between the latest scan and what your patching solution is telling you. These are integrated into a single view of the asset in Verve.

But pure technology is not sufficient in OT. Third party apps usually require manual review of the vendor's website to look for new updates. One of our clients is currently monitoring just under 300 third party apps that fall in this category just at one facility. Fortunately, Verve leverages the scale we have across clients to provide a much lower cost solution than any individual company can provide on their own. Based on our software and firmware inventory gathered from Verve, we monitor for updates and patches. In addition, if the client has agreements with OEM vendors, we will integrate those approved patches into our source tool.

Filter and Assign to End Points

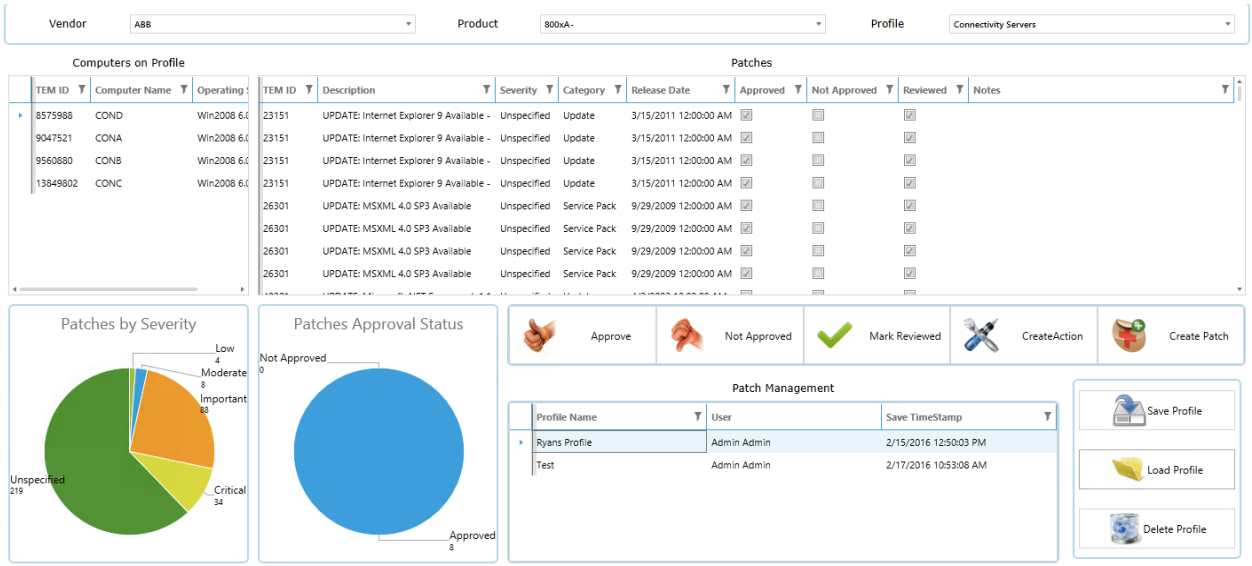
One of the most challenging elements of patching is to use the inventory to determine which assets should apply which updates – or filtering in other words. Verve Patch allows the client to automatically filter on the specific assets that are in scope for a particular patch. Verve can sort by any number 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. Again, if a client has a subscription to OEM

VERVE INDUSTRIAL PROTECTION

vendor approved patches, we can integrate those and also identify which critical patches might have been excluded by the vendor.

Patch review/approval/mitigation

Many processes end there and leave the approval and action to another set of tools or processes. Verve Patch brings the approvals and actions right into the same toolset. Verve Patch 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. Further, the user can sort on patches approved by the vendor and those that are relevant but not approved by the vendor. This allows full transparency into the full vulnerability and patch picture, not just what is approved by any individual OEM.



Testing and Deployment of Patches

Patch testing is standard in IT, but even more critical in OT. Verve enables testing by automating deployment to a series of test devices, monitoring their performance through the Verve Event Manager, and then enabling the user to take the next step of programmatically deploying patches across OEM Windows/Unix/Linux devices right from the console. It can then roll-back updates that are not working appropriately. Then the additional roll-out can be scheduled at any sequence. Importantly, Verve also integrates backup information, so that before you patch, you can be certain that a recent, quality backup exists for the machine. Additional controls such as control over automatic rebooting of 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 deployed in an automated fashion – such as embedded devices, we offer professional, experienced staff who will come on site on a regular basis to deploy those firmware updates. 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 & Documenting Systems Pre/Post Patch

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. Our agentless based solution extends this same change management function to embedded devices providing compliance and new baseline information for OT devices which do not support an agent, without waiting for a passive sensor to pick up the change on a wire.

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

The Verve Patch module, integrated in the Verve Security Center, along with VIP services provides an end to end solution to the challenges of patching in industrial control systems. In summary the combination of technology + talent allows for:

- ✓ Lower cost to identify and assign appropriate patches and updates
- ✓ No risk vulnerability assessments with no aggressive vulnerability scans
- ✓ Less complex and burdensome gathering of compliance required data
- ✓ Ability to patch and update even remote embedded devices leveraging expert ICS resources
- ✓ Less risk with robust testing methodology and expert services

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.

VERVE INDUSTRIAL PROTECTION