Technical White Paper

OT END POINT PROTECTION

Verve Security Center offers a complete solution for End Point Protection, specifically design for Operating Technology in Industrial Control Systems

End Point Protection in OT

End point protection is a critical element of all cybersecurity programs, but has traditionally been hard to execute in industrial control systems (or operating technology) environments. Leveraging our 25-year experience in ICS engineering from our parent company, RKNeal Engineering, Verve Industrial Protection has built an end-point protection solution that addresses the unique criteria and challenges of OT environments. This paper summarizes that solution.

OT End-point Protection: The Challenges

OT End-point Protection is a necessity to protect the world's infrastructure, but in many cases it is not deployed due to several key challenges. Several unique characteristics of these networks and the processes that they control make running traditional end-point protection solutions very difficult if not impossible.

- The vast majority of devices in an OT network do not run Windows/Unix/Linux but instead operate on ICS equipment OEM protocols with no ability to deploy traditional IT agents.
- Even those devices that are Windows-based are designed to integrate in highly customized control system networks making third party management difficult for those without deep experience in those systems.
- Processes that these systems control are much more sensitive than traditional IT processes – for instance, you cannot just reboot your turbine controls when you run an update without risking shutting down an operation for a long period of time
- Many of these systems operate in remote environments that require a low cost, easy to use solution
- Updating & patching requires accessing hundreds of non-IT applications and OT vendor websites to determine whether an update exists and what the scope of that update is (e.g., Schweitzer relays or Hirschmann switches). Then once this is determined, the process is usually a slow manual effort of visiting each device with a memory device to upload the update.
- The solutions that are offered today are mostly from the OEMs themselves, leading to a patchwork for solutions across a corporate OT network with each OEM managing their own equipment but a lack of visibility across entire network.

As a result of these challenges, end point protection management is hugely time-consuming or is just simply not done.

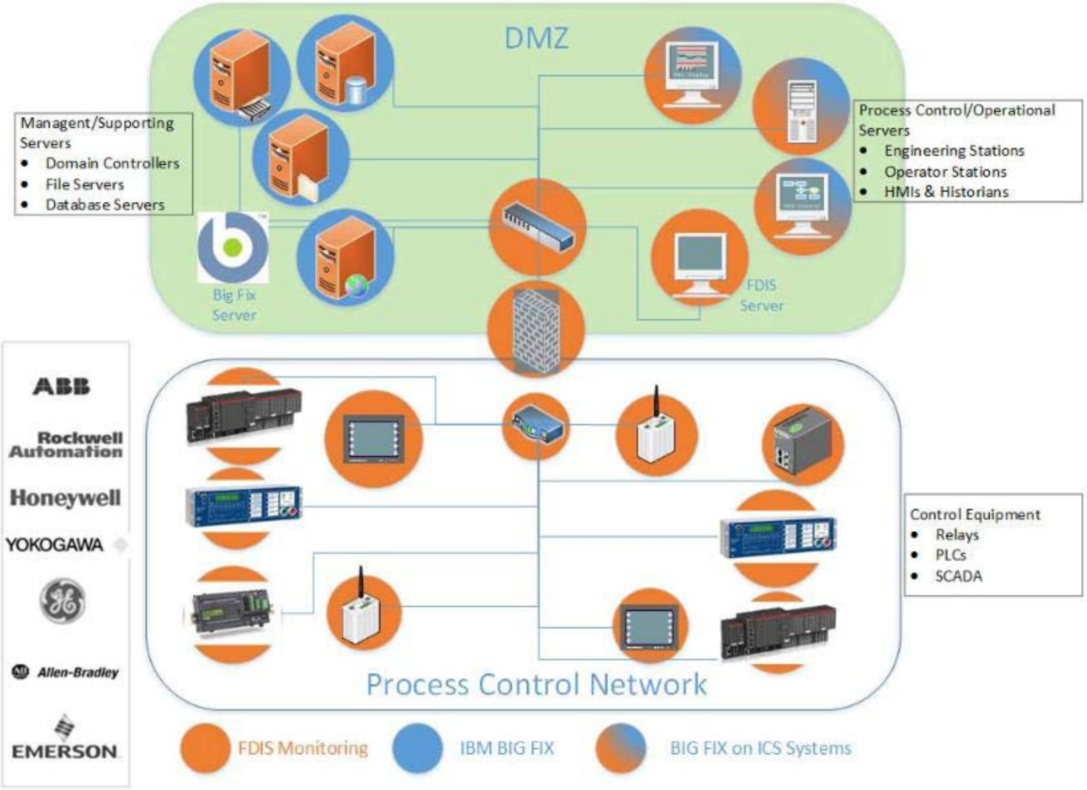
OT End-point Protection: The Solution

Because of these challenges, we have leveraged our 20+ years of ICS engineering experience as RKNeal Engineering to build Verve Industrial Protection (VIP) – a division focused specifically on OT cybersecurity. Our Verve Security Center (VSC) software and our Verve Industrial Protection Services (VIP Services) deliver a complete OT end point protection platform that addresses the complexities discussed above.

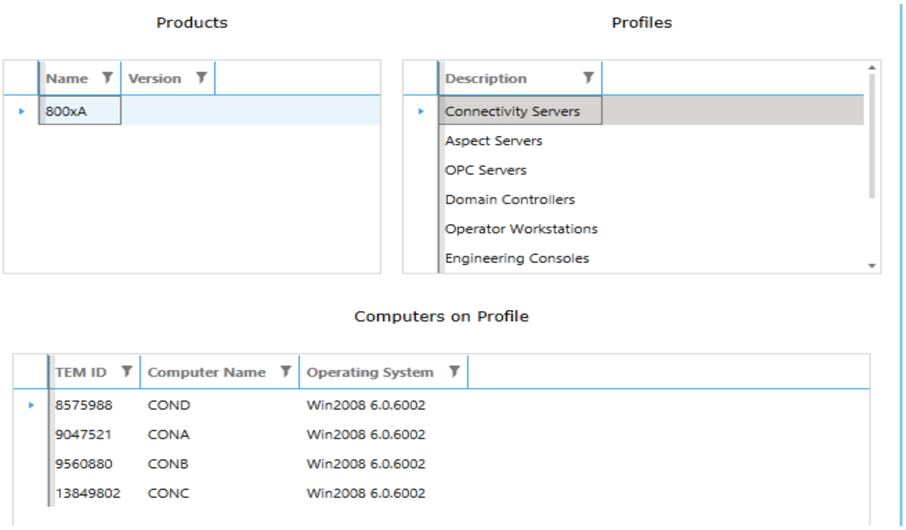
VSC is the only solution of its kind that is built ground-up with Industrial Control Systems in mind. As a team we have operated plants, deployed Emerson, ABB, Rockwell, and many other control systems. And we have seen the challenges these systems present. Therefore, VSC embeds this knowledge to create a solution that is safe, effective and efficient for OT end-point protection.

VSC includes 6 critical elements:

1. A best-in-class agent-based solution selected because of its flexibility for customization, its lightweight footprint, its scalabililty, and ease of use. This is the IBM BigFix agent. We then apply VIP-customization of the way the agent operates so that it is configured to work across all OEM vendor equipment without disruption (proven by over 8 years of operating in plant environments) to provide a single solution across vendors.
2. A proprietary Verve Industrial Protection solution – our Foreign Device Information Service (FDIS) - that extends BigFix into the unmanaged assets of relays, RTUs, IEDs, PLCs, etc. to gather configurations and other asset information from these proprietary protocols so that a user can see and managed 100% of their assets.



3. A low-cost, scalable architecture leveraging proprietary software to reach remote locations efficiently – and one that enables auto-identification of new devices as they are added to the network
4. A user-interface which brings together all of this information into a searchable and automated asset management system to provide full visibility and actionability.



Products

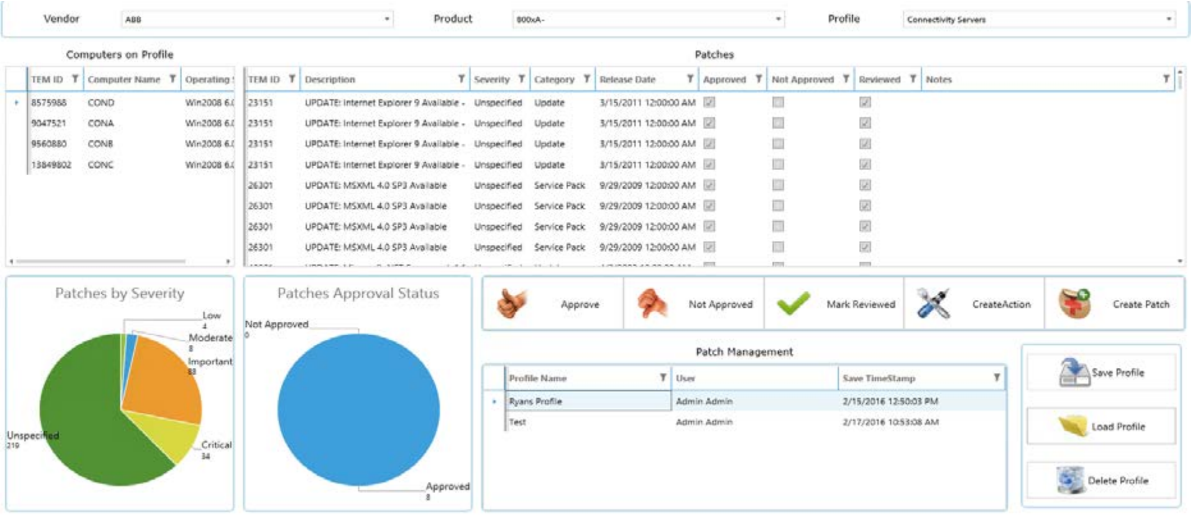
Name	Version
800xA	

Profiles

Description
Connectivity Servers
Aspect Servers
OPC Servers
Domain Controllers
Operator Workstations
Engineering Consoles

Computers on Profile

TEM ID	Computer Name	Operating System
8575988	COND	Win2008 6.0.6002
9047521	CONA	Win2008 6.0.6002
9560880	CONB	Win2008 6.0.6002
13849802	CONC	Win2008 6.0.6002



Vendor: ABB
Product: 800xA-
Profile: Connectivity Servers

Computers on Profile

TEM ID	Computer Name	Operating S
8575988	COND	Win2008 6.(
9047521	CONA	Win2008 6.(
9560880	CONB	Win2008 6.(
13849802	CONC	Win2008 6.(

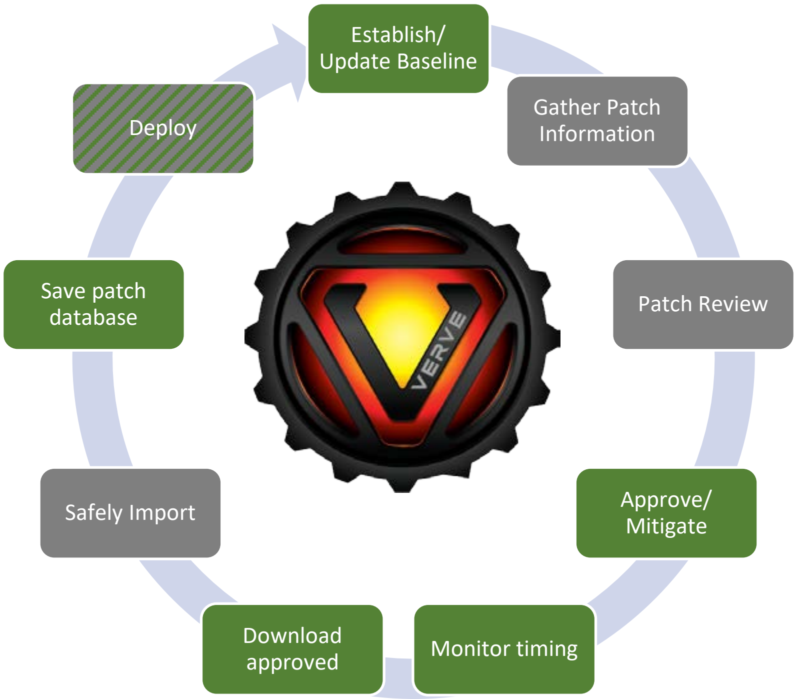
Patches

TEM ID	Description	Severity	Category	Release Date	Approved	Not Approved	Reviewed	Notes
23151	UPDATE: Internet Explorer 9 Available -	Unspecified	Update	3/15/2011 12:00:00 AM	☑	☐	☑	
23151	UPDATE: Internet Explorer 9 Available -	Unspecified	Update	3/15/2011 12:00:00 AM	☑	☐	☑	
23151	UPDATE: Internet Explorer 9 Available -	Unspecified	Update	3/15/2011 12:00:00 AM	☑	☐	☑	
23151	UPDATE: Internet Explorer 9 Available -	Unspecified	Update	3/15/2011 12:00:00 AM	☑	☐	☑	
26301	UPDATE: MSXML 4.0 SP3 Available	Unspecified	Service Pack	9/29/2009 12:00:00 AM	☑	☐	☑	
26301	UPDATE: MSXML 4.0 SP3 Available	Unspecified	Service Pack	9/29/2009 12:00:00 AM	☑	☐	☑	
26301	UPDATE: MSXML 4.0 SP3 Available	Unspecified	Service Pack	9/29/2009 12:00:00 AM	☑	☐	☑	
26301	UPDATE: MSXML 4.0 SP3 Available	Unspecified	Service Pack	9/29/2009 12:00:00 AM	☑	☐	☑	

Patch Management

Profile Name	User	Save TimeStamp
Ryans Profile	Admin Admin	2/15/2016 12:50:03 PM
Test	Admin Admin	2/17/2016 10:53:08 AM

5. VIP Services “Closed-loop update service” that on a monthly basis accesses and reviews patches & updates from hundreds of OT apps and vendors to identify those that are security related, and then integrates those into VSC for automated deployment on our client’s networks. This patch management is done across vendors so that users do not need to manage multiple vendor’s systems.



6. Optional OT-specific application whitelisting using the best-in-class whitelisting product from Bit9/Carbon Black. We have applied our years of experience across every major OEM system to develop the necessary customization for each OEM to ensure our clients can truly lock-down the whitelisting.

Verve Security Center: The Benefits

The result is a solution that not only delivers true end-point protection for ALL of your OT assets, but does so safely, effectively, and efficiently. Key benefits include:

1. **Lower total cost of ownership.**
   Because VIP operates across vendors and integrates the various elements of end-point protection into a single offering, the cost to deploy and most importantly the labor costs to manage the protection is significantly reduced.
2. **"OT Safe"**
   We have embedded over 20 years of industrial controls engineering into Verve Security Center. Before we focused on security, we focused on safety & reliability. We understand that in many cases, companies in the pursuit of security have actually made their systems less reliable. VSC starts from the premise "first do no harm" and we embed that mindset into all elements. We have had VSC operating on industrial environments for over 8 years with no disruption of operation for our customers.
3. **Greater network visibility**
   In many cases before deploying VSC, our clients we using Excel spreadhseets or Access databases manually updated to keep track of their OT assets. VSC enables automated asset identification, inventory, and management – across ALL OT assets, not just the Windows boxes.
4. **Reduced complexity of managing updates**
   With our VIP Closed-loop update service, we take the headache out of patch management by bringing our scale to update identification and review combined with the automation of Verve in scheduling and deploying patches when and where you want.
5. **More secure networks**
   Because of this complete view of configuration changes, patch status along with the ability to deploy updates regularly – and in many cases combined with our optional OT application whitelisting – our client's networks are fundamentally more secure than they would be otherwise.

***

We would be happy to provide more material or a demonstration of VSC and its capabilities at any time.