VERVE
INDUSTRIAL PROTECTION

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

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

End Point Protection in OT

End point protection is a critical element of all cybersecurity programs. However, security management such as patch and vulnerability, configuration, software, user and access as well as protective measures such as AV and Application Whitelisting is difficult in Operating Technology environments. Leveraging our 25-year experience in ICS engineering, Verve Industrial Protection has built the only OT-focused end-point management & protection solution in the market. 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, Verve has leveraged its 25 years of ICS engineering experience to build the Verve Security Center (VSC) to deliver a complete OT end point protection platform that addresses the complexities discussed above.

VSC is the only end point management & protection solution that is built ground-up with industrial control systems in mind. Our team has operated plants, deployed Emerson, ABB, Rockwell, and many other control systems, and has 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.

VAM includes 6 critical elements:

1. A best-in-class agent-based solution with a lightweight footprint that is configured to work across all OEM vendor equipment without disruption (proven by over a decade of operating in plant environments) to provide a single solution across vendors.
2. A proprietary Verve Industrial Protection agentless solution that extends our asset visibility and protection 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. Verve Patch & Vulnerability Manager which provides an end-to-end automated patching solution that 1) identifies vulnerabilities & patch availability, 2) automatically defines which patches are relevant for which devices, 3) automates a significant part of deployment, and 4) integrates all compliance monitoring and reporting into a single user-interface.
4. Verve End Point Protection: A comprehensive suite of OT-focused end point protection that includes AV, Application whitelisting and removable media protection, as well as host-based intrusion detection.
5. Verve Security Center Reporting: A user-interface which brings together all of this information into a searchable and automated asset management system to provide full visibility and actionability.

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.