



AN INTERVIEW WITH TOBY WEIR-JONES
CHIEF PRODUCT OFFICER, BAYSHORE NETWORKS

ACTIVE OT SECURITY VISIBILITY & MITIGATION

THE first goal in protecting operational technology (OT) is to recognize that the connectivity of your industrial environment has probably expanded far faster than your growth in staffing and expertise required to protect your plant. As a result, you now have a very basic safety problem: lots of risk, and no practical ability to mitigate it.

This is not a matter of assigning blame. It's a simple resourcing issue. There are very few skilled industrial network security analysts, and those who are available are in huge demand. They command enormous price tags and have the luxury of endless career mobility, even in the hottest job markets nationwide. If you're a regional operator, the chances of finding one of these professionals – or training and keeping one in-house – are very slim.

Bayshore Networks has developed a commercial solution that resides inline on the OT network and provides real-time inspection and protection of OT assets and activity. Rather than offer it as a single monolithic solution, the company has divided it up into tactical point solutions for specific use cases, allowing customers much more straightforward evaluation and budgeting requirements while slowly building up the installed base. We recently met with Toby Weir-Jones of Bayshore Networks to learn more about OT active mitigation from cyber threats.

EA Do you still have to convince OT companies that they need to focus on cyber security?

TWJ Most operations technology (OT)-oriented companies now recognize that they need to pay close attention to cyber security issues, but the challenge is they're not sure exactly where to start. They're being bombarded by complicated product messages without a lot of clear thought leadership on best practices. We've adjusted our focus towards a core set of critical OT security activities which should be monitored in every OT environment, along with recommendations on what mitigation steps can be performed without disrupting operations or safety.

EA Where should an OT security professional focus their efforts?

TWJ They need to understand not only what's "out there" on their networks, but also what they can do, safely and constructively, to improve their OT security within the safety and maintenance parameters that production environments demand. Improvements in configuration, or network segmentation, or policy can often be done without requiring downtime on the floor, and Bayshore is the only ICS security tool which can provide real-time mitigation to protect OT devices at the payload level. This allows safer operation, with less downtime, all while improving your security posture.


EA Tell us how your solution works and how it can be used for visibility and mitigation?

TWJ Bayshore offers three products oriented around the same core engine. That engine understands and decodes a wide range of native OT network protocols, at wire speed, with incredibly low latency. It lets us get all the way down into the last bits of payload, make decisions on a whole range of risk factors, and return permitted packets back to the wire. The first product using this is called SCADAFuse.

It sits right in front of a PLC and acts as the last line of defense. If traffic from unauthorized sources, or of unauthorized types, or at unauthorized times, tries to touch the PLC, SCADAfuse prevents it and sends an alert to the operator's control room – their SCADA HMI – via a built-in modbus server. It can be set up in 15 minutes, evaluated for purpose in a week, and costs less than a week's worth of field engineering time for a single automation technician. The second product is our remote access solution, called OT Access. It's available as both a hosted solution (for managed service providers or other cloud-friendly deployments) and a fully on-premise version. It is designed to provide access control to OT assets with the absolute minimum exposed connectivity, along with the same content inspection and policy enforcement using the Bayshore policy engine. The third product – SCADAwall – is designed to take the traditional hardware data diode and make big steps forward on value and flexibility. It provides the same core feature – non-repudiable data transmission across the diode – but with live file object capture and inspection, for malware, OEM hash checking, and known ICS CERT vulnerabilities.

EA What trends are you seeing in OT security, other than perhaps greater awareness?

TWJ The customers have been flooded with visibility pitches for the past few years, and they are realizing that awareness is only the very first part of an effective OT security solution. Ultimately, they need to know what to do next, and how much of that can be done on their behalf by their tool or their service provider. OT threat mitigation is all about preserving production safety and continuity unless you absolutely can't, and then providing the best detail and recommendations so everyone has a transparent and objective understanding of why the OT team needs organizational support for major risks. The vendors who will succeed in this evolving space are already positioned to enable these 'shades of gray' and satisfy the demands of not



Improvements in configuration, or network segmentation, or policy can often be done without requiring downtime on the floor.

only the OT security team, but the corporate IT security team as well.

EA Any new features or capabilities that your team is currently working on?

TWJ Absolutely. Bayshore's strategy is to bring its payload-level policy controls to the entire OT environment. This includes the network inside the plant, the transition layer to other corporate or external networks, and the remote access gateway required for trusted ingress. With the three products I mentioned above, it's an exciting time to invest in the Bayshore platform and we are confident our solutions will readily distinguish themselves from the visibility and asset management providers on the market today.