# CIOCoverage

Driven For Technology Leaders

10 Fastest Growing

CIOCoverage

## CYBER SECURITY SOLUTION PROVIDERS 2021

# BAYSHORE NETWORKS

## Spanning the Cyber Risk Gap

**Kevin Senator**
*CEO*

CIOs with responsibility for securing production plants and factories would agree that there never seems to be sufficient human capital to secure, manage, and respond to safety and availability requirements of industrial networks and control system endpoints used to produce their company's goods and services for our world. What's needed is the ability to apply active protection to support Operations Technology priorities and limited resources.

Cybersecurity risks in plants and factories have been there for decades, but these facilities adopt change cautiously and slowly. However, industrial networks are becoming much less insular and more interconnected, and therefore susceptible to threats from both outside and inside that can impact safety and productivity.

10 Fastest Growing CIOCoverage CYBER SECURITY SOLUTION PROVIDERS 2021

BAYSHORE NETWORKS
INDUSTRIAL AND IT NETWORK SECURITY

Bayshore Networks has dedicated its resources since 2012 to bridge the security and protection gap that exists in most industrial and critical infrastructure production networks and control systems. Most CIOs have expert security teams who can secure, manage and respond to enterprise needs. But, the competence needed to understand OT networks and devices is usually lacking, despite strong security skills in the CIO's team. This is because OT networks have a whole different set of priorities and requirements and enterprise security tools are mostly inappropriate for OT networks.

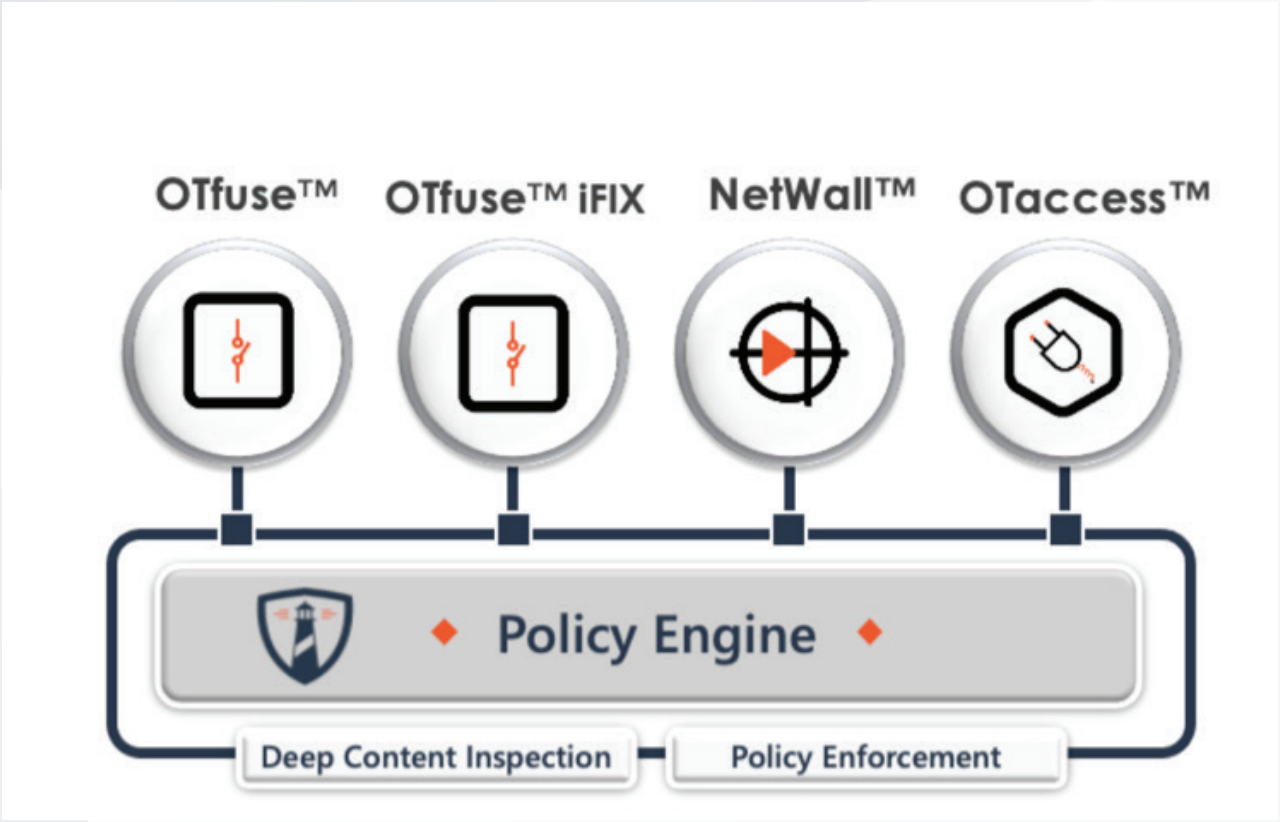
As an example, COVID-19 has caused IT organizations to prioritize worker safety and effective remote access above many other projects. In OT environments, the quick IT "fix" of widely deploying Virtual Private Networks (VPNs) for access into plant networks does not adequately protect the industrial control systems (ICS) that the remote workers need to access. Once through the VPN, a remote employee or trusted contractor can typically get to every system within the production factory due to existing security gaps.

A better solution, and one Bayshore Networks has pioneered, is to provide OT-friendly, enforceable hardware and software policies that will allow specific individuals access only to the devices they are authorized to interact with. This can be enforced per person, per protocol, per device, etc. The solution is called OTaccess™ and is compatible with VPNs and firewalls but takes a unique approach to add the essential layer of protection to ensure production continues uninterrupted.

When malware or ransomware hits a business, it can be catestrophic to both the IT(corporate) and the OT (plant) sides of the business. A plant which cannot continue production due to systems which are locked up and unable to function has huge financial impact to company profits. Often, recovery is a long and painful process if adequate security and protective actions were not taken in advance. Commonly, IT teams have a big scramble on their hands to understand how to assist their plants and factories with recovery, and it can sometimes take many months to gain back what was lost.

"We build a risk-based approach into everything we provide our customers," said Bayshore's CEO, Kevin Senator. "We provide an affordable, modular ICS security platform that is designed from the bottom up to make it easy and effective for OT environments. Bayshore can augment limited OT staff, and we deploy security and protection without production downtime, using a risk-based approach in alignment with OT priorities of safety, availability and no impact on operations."

Bayshore Networks offers OTfuse™ to provide cabinet-level protection for programmable logic controllers (PLCs) and other process control devices, OTfuse for GE Digital iFIX and Cimplicity environments, NetWall™ for patent-pending, high performance, one-way data transfer out of the plant with network




*Bayshore Networks Modular ICS Platform*

segmentation protects sensitive plant assets from attack and downtime, and OTaccess to secure remote access to industrial assets.

Bayshore provides its technology strictly through its global partner channel network. As a go-to-market strategy, this approach has enabled a relatively large global footprint. “In 2020, we went from 3 channel partners in North America to recruiting over 20 channel partners globally – far exceeding our growth targets,” said Senator. “This indicates there is keen interest in adding protective security to plants and factories worldwide.”

One of the Bayshore customer case studies is a personal goods manufacturer who sought to achieve better efficiency by standardizing on OTaccess as the means by which they allowed employees, industrial equipment manufacturers, contractors, supply chain and others to access to plant assets. Aside from efficiency gains, this customer also experienced significant cost savings they estimate to be approximately one full-time employee’s salary each year per plant.

What is needed is easy deployment and usability for operators, self-learning technology, and protective response at machine speeds.

## Given the current cyber threat landscape, and existing cyber risks in most plant and factory environments, it's definitely not good enough to accept "doing nothing" any longer.

Compounding these cost savings over time, they are continuing to roll OTaccess out to all plants worldwide.

In regard to OTfuse for GE Digital (GED) iFIX and Cimplicity, Bayshore Networks was uniquely qualified to work with GED's development teams to build in protective security support layers for specialized protocols GED uses in communication between its human machine interface (HMI) and supervisory control and data acquisition (SCADA) assets.

The industrial threat landscape is constantly evolving, just as it has for so many decades in the enteprise side, said Senator. "Industrial companies have to adapt and keep working to protect and secure their networks and assets. You can't stand still."

Mr. Senator adds, "What is needed is recognition that plant environments – networks, devices, and endpoints are not at all the same as on the corporate side. OT teams need easy deployment and usability for operators, self-learning technology, and protective response at machine speeds. Though smaller and mid-sized organizations will likely never have the headcount and operational security expertise of larger organizations, it's definitely not good enough to accept "doing nothing" any longer, and especially when Bayshore's solutions are designed, field-tested, and proven to affordably address these exact needs."