



BAYSHORE NETWORKS
INDUSTRIAL NETWORK SECURITY

Field Application

Case Study: Securing Supply Chain Remote Access *(and others)*

Global Personal & Consumer Goods Manufacturer
USA

BACKGROUND

The customer is a Fortune 500 American manufacturing company with revenues over \$NN billion. It manufactures household and commercial consumer goods and is over 100 years old. Its products are sold and manufactured around the world and are in the number one or two position in a majority of its markets.

The company began a supply chain process renovation which was designed to reduce distribution costs and build the capacity to better serve its sales outlets at every stage. They had a heterogenous OT environment with a mix of manufacturing vendor equipment. By 2017, they had identified additional needs for securing remote access for their supply chain partners, industrial equipment manufacturing vendors, trusted contractors, and employees.

CHALLENGES

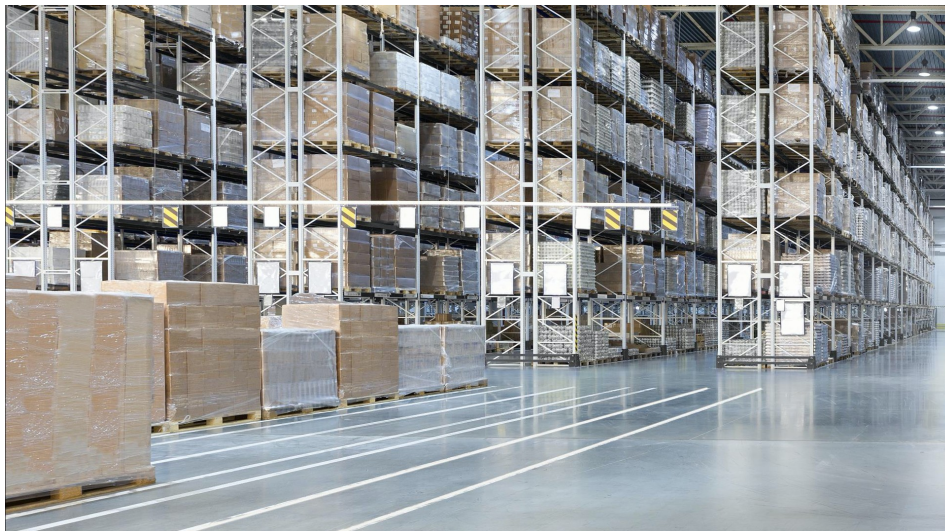
When the customer began its supply chain partner reorganization, the original objective was to better serve retail customers by delivering their personal care and consumer products to retail shelves faster, particularly during promotional campaigns, to help maximize sales. During this process they also identified a maintenance need to allow contracted industrial equipment manufacturing vendors access to specific industrial equipment.

The challenge with third parties was that each one had their own approach to accessing the network, equipment and access tools. The upkeep on giving and maintaining access for all the vendors - added to the supply chain partners had become a maintenance nightmare. Further, there was no real governance on what systems these third parties could access once authenticated for access in the relatively flat production network. The OT team wanted a solution they could control and enforce without needing to go through corporate IT.

With the advent of COVID-19 in 2020, the company added a bigger list of remote users to those needing access to the plant network and assets. Many of these personnel were in the category of high health risk due to age and other factors. The company's first concern was employee health and safety, but they also had to acknowledge that these resources were not easily or quickly replaceable should the need occur, so remote access for home workers became a top priority.

The customer developed a short checklist of requirements to begin the search for a technology partner to help shore up security gaps and help them have a single method, applicable to many types of authorized, remote access users for whom OT wanted to govern and enforce policy:

- ▶ **A solution that OT could manage to handle ongoing requests for remote access to plant resources**
- ▶ **Deployment options for virtualized server or physical machines**
- ▶ **Willingness to consider cloud for faster implementation and ease of maintenance**
- ▶ **Ability to apply accountability and control, managed centrally**
- ▶ **Unified access to specific OT assets**
- ▶ **Policy creation and global enforcement**



SOLUTION AND DEPLOYMENT

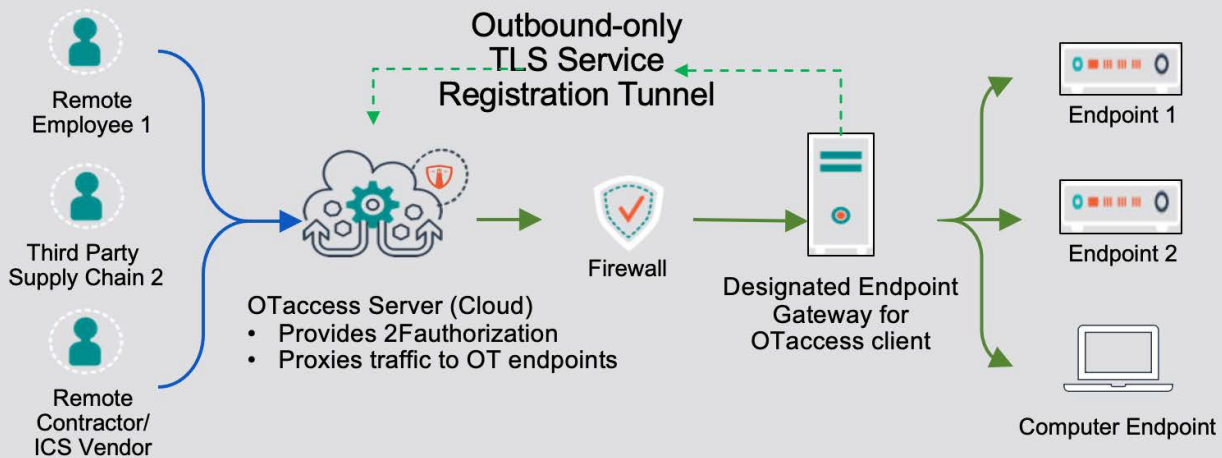
The company issued a Request for Proposal (RFP) and Bayshore Networks OTaccess™ was selected as the winning solution design. A virtualized instance was quickly deployed and made available to the customer's largest plants, in conjunction with the Endpoint Gateway™ software solution inside the plant's OT network perimeter. They were then able to document and publish an efficient, consistent process for remote access with third party supply partners, industrial vendors and at-home workers. They were also able to determine and enforce granular policies around permitted asset ACLs, user activity monitoring and enforcement, and protocol-specific continuous content inspection of user sessions.

Reference Deployment Architecture

In the early stages of deployment, the plant engineering team were surprised that once they'd completed their preparatory information needed, the initial implementation with a starting small set of users took place in less than an hour.

The preparation required was to open firewalls outbound, install the endpoint gateway (as simple as installing the Bayshore app on an existing PC), and setting up users. In this manufacturer's requirements, there was also later interest to include options such as Active Directory and two-factor authentication which required details from corporate IT.

OTaccess™ Deployment Architecture



BENEFITS & EXPANSION PLANS

The manufacturer has a standard, centralized remote access solution for all OT use cases, instead of having to manage a wide array of different solutions with different capabilities and degrees of integration with other corporate resources.

Cost Savings

Given global operations, and further expansion of the user base, the customer will continue to double its year-over-year growth of active users with thousands of additional connections for the foreseeable future.

The customer savings they estimate to be approximately 1.5 full-time employee equivalents annually per 2-3 manufacturing sites active in the system. The savings will be further expanded as they increase usage over time and are able to easily scale to the growth.

This was achieved due to the process improvement and reduction in IT and OT management overhead by standardizing on a single remote access solution. Additionally, the technology alleviated any disturbance to the process while still being able to block usage violations in real time without incident escalation and response.

Benefits to Plant Operations Technology (OT)

- ▶ Increased efficiency and supported OT process improvements while ensuring safe, cybersecure access for remote users to access plant resources.
- ▶ Reduced attack surface and easier maintenance of users, permissions, and allowed changes enforcing consistent behaviors through policy related to remote access.
- ▶ Improved cybersecurity through granular OT control over each user, protocol, and system accessed along without unnecessary burden on OT personnel.
- ▶ Continuous content inspection throughout user sessions with the ability for an instant block (if desired) of illegal or unauthorized user activity in violation of content policy.
- ▶ Session recording available for RDP connections, beneficial in troubleshooting, and for records-keeping.
- ▶ Higher efficiency through being able to more quickly give approved users remote access without having to cycle through corporate IT.

"We have all these third parties who need access to their own equipment and we can't keep track of it all or manage it centrally. And on top of that, we have a huge number of remote workers who also need access to ICS and SCADA systems, but not access to everything. It's impossible to manage."

*- Operations and Plant Management,
Global household and commercial
goods manufacturer*

For more information and a discussion about your site needs,

Email info@bayshorenetworks.com.



BAYSHORE