INDUSTRIAL INTERNET IN ACTION **CASE STUDY**

Global Manufacturer uses remote access cybersecurity to maintain safety at its manufacturing production zones

EXECUTIVE SUMMARY

One of the world's largest manufacturers reduces production downtime and cuts costs by using cybersecurity to remotely monitor and enforce security in its factories. Designed and built by Bayshore Networks and its partners, the solution enables secure remote access with transaction control to factory production cell zones while ensuring zero downtime and higher availability of production systems. Using smart devices, employees and engineers at partner companies can now remotely troubleshoot problems in the factory from anywhere in the world.

> *"Robots have always been able to perform self-diagnostics. Now through the use of Cisco and Bayshore technology, we can securely transmit robot diagnostic data to a remote server for additional diagnostic analysis. Through the use of Bayshore security technology, we can control access to any level of the robot information."*
>
> - Director, Global Manufacturer Partner Organization

THE CHALLENGE

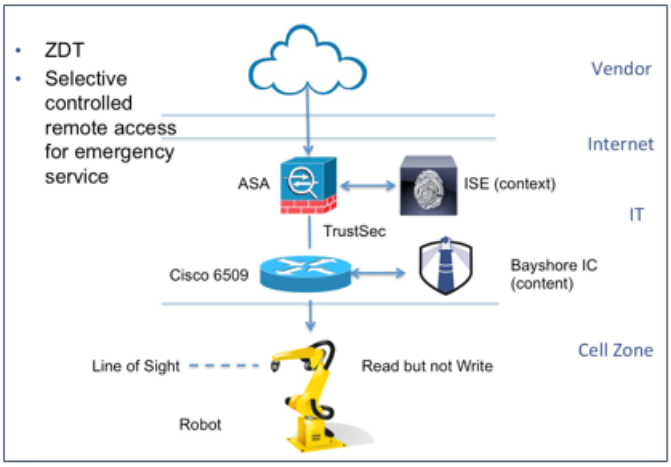
The client is one of the world's largest and most technically-advanced manufacturers in the world. Strict security guidelines meant that outside technicians were only allowed remote access to cell zones inside the factory to service the company's robots and assembly line monitors during emergencies. During these emergencies, the company's IT department gave technicians specific access over VPNs by opening several ports for manual entry into the factory systems.

This process did not enable the IT department to maintain its typically high standard of granular access control when the VPN ports were open. Access was provided on an exception basis, which severely limited the department's ability to establish persistent postures for cybersecurity and safety. The manufacturer required a solution that safely provided secure remote access with transaction control while ensuring zero downtime and higher availability of production systems.

THE SOLUTION

The company asked its engineering partners to work with Bayshore Networks and Cisco to design a solution that provided secure remote access that adhered to the company's safety and cybersecurity guidelines.

Bayshore and Cisco quickly determined that traditional network-style security wasn't adequate; the IT department also needed control over transaction semantics. This level of granularity required Bayshore IC's content-aware filtration capability. Bayshore IC technology inspects all transactions as they pass through the network at a very deep level, allowing operations that are safe and disallowing operations that aren't safe or may compromise plant safety.



Working in concert with Cisco ISE and ASA, the Bayshore IC solution enables secure remote access to cell zones while providing granular access control and meeting the IT department's zero downtime requirement.

Cisco provided the network security for encryption and partner/device identification, and Bayshore provided the transaction security. Bayshore solved the security problem of allowing remote access with line of sight control. Line of sight requires that any controls sent to a robot or machine must be executed by an operator who can physically see it. Machines move in physical space and can endanger the safety of operators standing near them. In the remote access solution, Bayshore IC enforced the line-of-sight rule through transaction-based security rules and content-awareness. This enabled Bayshore IC to distinguish which control signals are writes and which are reads. In this case, writes were disallowed and reads were allowed.

RESULTS

Today, engineers are using smart devices to troubleshoot problems in the factory, safely and securely from remote locations. The solution delivered secure remote access, giving the manufacturer and its partners the ability to perform diagnostics and maintenance with less travel and faster turnaround. By using remote line-of-sight access to assembly line robots, the company ensured they were managed safely and errors were avoided that were possible under the previous emergency VPN scenario, such as accidentally writing commands to robots. The manufacturer has cited benefits of this solution which include reduced downtime; more efficient management of outages; and enhanced operations.

About Bayshore Networks

Bayshore Networks is setting the standard for operational, safety and security policy for the Internet of Things. Our award winning, patented, industrial-strength cybersecurity platform is developed exclusively in the United States and is trusted by world leaders in Industrial Controls, Critical Infrastructure and Fortune 500s. The open, flexible Bayshore platform provides a foundation for organization-wide policy execution. It enables you to quickly deploy, evaluate and enforce industry standards and customized application-layer policies that drive your business objectives. Bayshore's core technology is Pallaton™, an embedded, extensible, XML-based policy language.

About the Industrial Internet Consortium

Bayshore Networks been a member of the Industrial Internet Consortium (IIC) since May 2014. The IIC is an open membership organization, with 135 members to date, formed to accelerate the development, adoption and wide-spread use of interconnected machines and devices, intelligent analytics, and people at work. Founded by AT&T, Cisco, General Electric, IBM and Intel in March 2014, the IIC catalyzes and coordinates the priorities and enabling technologies of the Industrial Internet. Visit www.iiconsortium.org.