

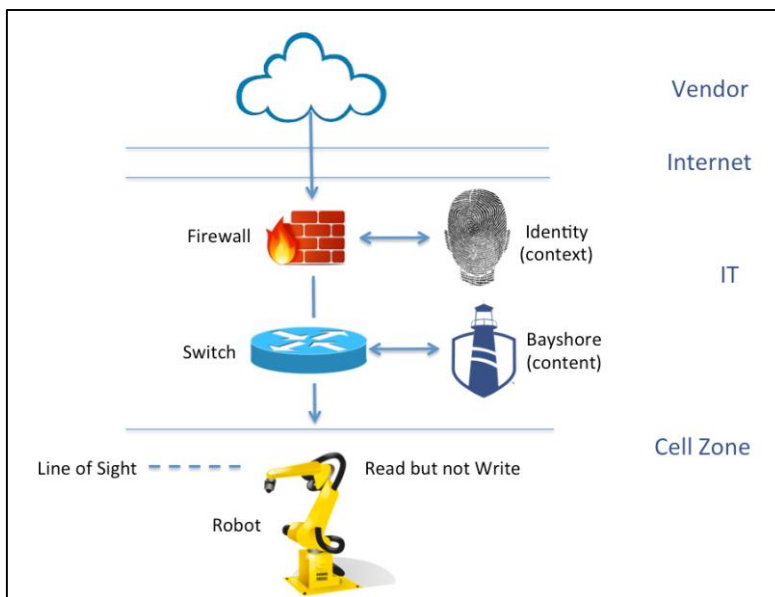
Global Automaker uses remote access cybersecurity to maintain safety at its manufacturing production zones

EXECUTIVE SUMMARY

One of the world’s largest automakers relies on Bayshore Networks’ IT/OT Gateway software technology for remote access cybersecurity and safety of its manufacturing production zones.

THE CHALLENGE

In the world of manufacturing, an unplanned outage typically requires technicians to be onsite to troubleshoot problems. But these experts usually work for partner companies and may take more than 24 hours to arrive onsite, leading to costly outages and production delays. To address the problem, one of the world’s largest automakers – widely considered one of the most technologically forward-looking organizations in all of manufacturing – asked Bayshore Networks and its partners to design and build secure remote access to its factory production cell zones.



The Bayshore IT/OT Gateway enables secure remote access to cell zones while providing granular access control and meeting the IT department’s zero downtime requirements.

Due to the IT department’s strict security guidelines, the partners – which provide engineering solutions such as robots and electronic controllers for assembly line conveyor belt motors – were typically only allowed to remotely access cell zones during emergencies. During these emergencies, they were granted access over VPNs. The IT department would open several ports and manually allow users to enter.

Of course, the open VPN ports did not enable the IT department to maintain its typically high standard of granular access

control. Access was provided on an exception basis, crippling 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 automaker asked its engineering partners to work with Bayshore Networks to design a solution that provided secure remote access that adhered to the company's safety and cybersecurity guide-lines. The resulting solution ensured that remote users would have line-of-sight access to assembly line robots to ensure they were managed safely. At the same time, the solution prevented potentially downtime-impacting actions that would have been allowed in the emergency VPN scenario, such as accidentally writing commands to robots. Thanks to Bayshore's IT/OT Gateway software technology, engineers at partner companies can remotely troubleshoot problems safely and securely from smart devices.

"Through the use of Bayshore security technology we can control access to any level of the robot information."

- Francis Cianfrocca, Founder & Chief Scientist

"There are several components to the problem of remote access and that is why we needed a partnership approach," explains Bayshore's Founder & Chief Scientist Francis Cianfrocca. "Several proven technologies came together in a novel framework that solves the problem of secure remote access with safety. And this enables high-value applications like zero downtime and delivers that value to the customer."

Bayshore 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's content-aware filtration capability. The Bayshore IT/OT Gateway software 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.

Transaction security required knowledge of custom and proprietary protocols. Here, Bayshore's extensible policy creation capabilities made the difference, making it easy to capture the required semantics of the application to meet the security objectives. "Robots have always been able to perform self-diagnostics," says a director at a key partner organization. "Now through the use of 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."

RESULTS

According to Cianfrocca, the manufacturer committed to the solution because the Bayshore IT/OT Gateway solved the security problem of allowing remote access with line of sight control.

“That was the main thing for them,” he recalls. “And we proved it with zero risk and convinced them the product could do what we said it would do.”

Line of sight requires that any controls sent to a robot (or any 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 enforced the line-of-sight rule through transaction-based security rules and content-awareness. This enabled Bayshore to distinguish which control signals are writes and which are reads. In this case, writes were disallowed and reads were allowed.

The secure remote access technology has numerous business advantages in terms of the company’s bottom line – reduced downtime, more efficient management of outages, and enhanced operations. Secure remote access provides the ability to perform diagnostics and maintenance with less travel and faster turnaround.

“That’s the reason you have networks in the first place, so you don’t have to be there. So it totally cuts downtime and it cuts costs.”

- Francis Cianfrocca, Founder & Chief Scientist

ABOUT BAYSHORE NETWORKS®

Founded by a team of experts with deep roots in industrial controls (OT) and cyber security, Bayshore Networks’ breakthrough technologies enable safe and secure integration of IT and OT networks, systems, data, and infrastructure. Bayshore technology addresses the IT/OT Convergence Gap by creating a secure gateway between operational and business networks, protecting operational assets from internal and external cyber-threats while allowing operational data to be safely shared with business systems for monitoring, analysis, and other innovative business applications. For more information, please visit <http://bayshorenetworks.com>.

ABOUT THE INDUSTRIAL INTERNET CONSORTIUM

Bayshore Networks has been a member of the Industrial Internet Consortium since May 2014. The Industrial Internet Consortium is a global, member supported organization of over 250 members that promotes the accelerated growth of the Industrial Internet of Things by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data using common architectures, interoperability and open standards to deliver transformational business and societal outcomes across industries and public infrastructure. Founded by AT&T, Cisco, General Electric, IBM and Intel in March 2014, the Industrial Internet Consortium catalyzes and coordinates the priorities and enabling technologies of the Industrial Internet. Visit www.iiconsortium.org.

© 2017 The Industrial Internet Consortium logo is a registered trademark of Object Management Group®. Other logos, products and company names referenced in this document are property of their respective companies.