ovum

On the Radar: Bayshore Networks protects the Industrial Internet of Things

IT/OT Gateway blocks attacks and ensures machine efficiency and safety

Publication Date: 22 Feb 2016 | Product code: IT0022-000616

Rik Turner

Summary

Catalyst

Bayshore Networks provides security for industrial automation and control systems, a market commonly referred to as the Industrial Internet of Things (IIoT) or just the industrial Internet. Its flagship product is cloud-based gateway software that sits between information technology (IT) and operational technology (OT) networks to protect the latter from attacks originating in the former. By connecting OT data to industrial applications, Bayshore enables operational visibility and data transformation, which help provide actionable insight into OT processes and data.

Key messages

- The connection of industrial production environments to the Internet creates a requirement for cybersecurity.
- The place to deliver this is at the hand-off point between IT and OT systems.
- Bayshore does this with cloud-based gateway technology.
- Its policy and enforcement engine can handle the multiple protocols used in OT and extend to new ones thanks to its XML foundations.

Ovum view

The IIoT will continue to expand as more industries in more geographies see the need for connecting their machinery to the Internet to enable remote access. This will mean a growing requirement for cybersecurity products to protect machinery, and Bayshore will attract attention for its IT/OT cybersecurity capabilities.

Recommendations for enterprises

Why put Bayshore IT/OT Gateway on your radar?

If you are in the manufacturing industries, oil and gas, utilities, smart grid, or smart cities, and are connecting your machinery to the Internet, security must be a concern to you. Bayshore's technology should therefore be considered to deliver protection for your production environment.

Highlights

Ever more industrial machines are being attached either via an Ethernet connection or a satellite link to the Internet to enable remote access for diagnostics and troubleshooting, or to collect telemetry data on how they are performing. As a result, the PLCs, HMIs, and supervisory control and data acquisition (SCADA) systems used to communicate with and control them require protection from the multiple types of cyberattacks launched over the web. To this end, the Bayshore IT/OT Gateway sits at the TCP/IP hand-off point (the intersection of the IT and OT networks) to provide this security.

The company compares its product's role with that of a firewall in a traditional IT network, but whereas a firewall need only to look at IP addresses and the traffic on different ports, the gateway inspects machine application data and applies policy filters to it, which means it must be able to understand and parse comms protocols commonly used in the OT world, such as Modbus, to do its job.

The Pallaton policy creation and enforcement engine inside the gateways inspects and filters industrial protocols and applications down to the machine transaction level and is based on XML, which means it can adapt to new and proprietary protocols. This is important in industrial settings, because SCADA controls alone encompass hundreds of different protocols, many of them proprietary.

In particular, the Bayshore device must understand not only the syntax of these protocols, but also their semantics to avoid bogus control signals being fed into systems that could cause something to go offline or stop functioning correctly.

A common requirement for Bayshore customers is for the gateway to provide so-called line of sight, which means that someone at a remote site is allowed to log in and read information from a machine but not to write to it. This secure access enables functions such as remote diagnostics and predictive analytics while safeguarding the device from being tampered with.

Customers can deploy Bayshore technology either on-premise or in the cloud, but Bayshore says that customers are increasingly turning to the cloud. Intel, for example, deploys its IoT gateway on the customer premises, but there are fundamental differences. The Intel product is a low-powered, hardened physical device designed specifically for use on premises with IoT endpoints. Bayshore's IT/OT gateway is software-based, designed to provide security and policy enforcement for cloud-scale IoT deployments.

Background

Bayshore was founded in 2012 by its chief scientist Francis Cianfrocca, an expert in data security, computer-language design, compiler implementation, and network communications, and its VP of corporate development and finance, Bob Lam, who has held executive posts at J.P. Morgan and StrateSight Advisors, as well as shepherding funding for IT security firms such as McAfee, Symantec, ISS, and SonicWall.

Current position

After three years in the market with its product, Bayshore has built a global customer base of Fortune 10 and Fortune 100 companies in manufacturing, oil and gas, pharmaceuticals, and critical infrastructure, as well as serving customers in the government and military sectors.

Data sheet

Key facts

Table 1: Data sheet: Bayshore Networks

Product name	Bayshore IT/OT Gateway	**Product classification**	Gateway software
Version number	6.x	**Release date**	Q4 2015

Industries covered	Discrete and process manufacturing, oil and gas, energy/utilities, smart cities	**Geographies covered**	North America, Europe, Middle East
Relevant company sizes	Fortune 2000	**Licensing options**	Cloud, virtual, appliance
URL	http://bayshorenetworks.com	**Routes to market**	Direct, Channels
Company headquarters	New York, NY, US	**Number of employees**	Fewer than 100

Source: Ovum

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. Although On the Radar vendors may not be ready for prime time, they bear watching for their potential impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

Security Implications of the Internet of Things, IT0022-000277 (December 2014)

Author

Rik Turner, Senior Analyst, Infrastructure Solutions

rik.turner@ovum.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

no liability can be accepted in this regard – readers assume full responsibility and risk accordingly for their use of such information and content.

Any views and/or opinions expressed in this product by individual authors or contributors are their personal views and/or opinions and do not necessarily reflect the views and/or opinions of Informa Telecoms and Media Limited.

CONTACT US

www.ovum.com
analystsupport@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo