BAYSHORE

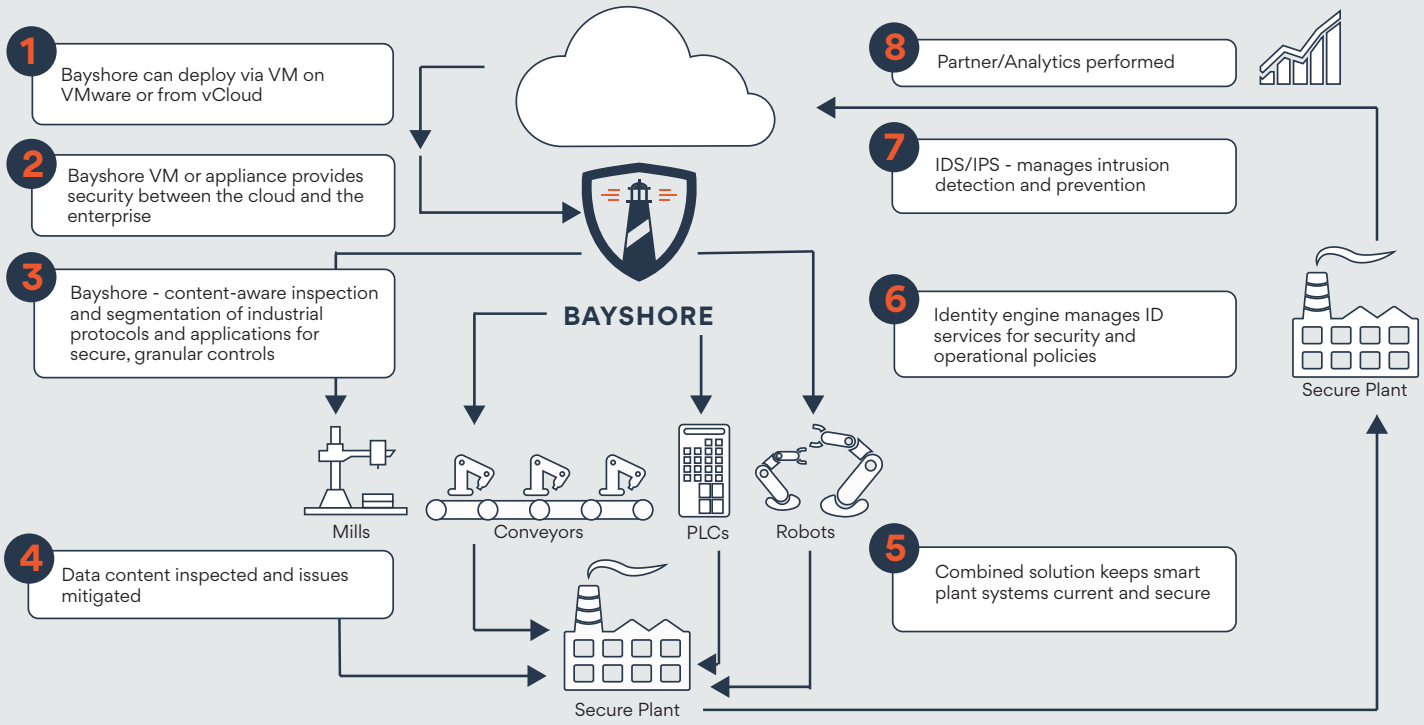
USE CASE

Auto Manufacturing

Today's manufacturing plants are unprotected from the Internet and vulnerable to cyber attack. Internet access to industrial robots, legacy OT networks and applications can drive significant economic benefits for manufacturers, but also create new security and operational policy vulnerabilities for legacy OT networks. Bayshore's technology provides native OT protocol and content-based cybersecurity to specifically address these vulnerabilities.

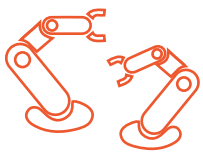
OT security has different requirements than IT security. Threats to OT networks and industrial assets include life safety, production downtime, operational disruptions and costly physical damage to equipment and products. In short, manufacturing networks require a completely different type of defense than IT networks.

Traditional perimeter firewalls provide a foundation for OT security but do not scale with massive manufacturing networks or provide security policy down to the data level. Bayshore translates industrial protocols down to the machine transaction level. This enables the extremely granular filtration, segmentation and isolation required to secure large-scale OT networks.



There are glaring business and technical shortcomings to deploying traditional IT security technologies such as next-generation perimeter firewalls in OT environments:

- Lack of industrial protocol and application domain knowledge required for OT networks
- Lack of granular deep packet inspection and application layer filtering capabilities required to enforce OT policies
- Lack of cyber-hardening capabilities
- Inability to provide security down to the machine transaction level, including data values
- Inability to scale effectively for large OT sensor networks
- Inability to tailor policies for safety standards or government regulations
- Inability to identify and prevent external or insider threats on OT networks.



*Every 3% production improvement leads to a **$600,000 profit increase** per day per plant.*

Bayshore enables the Industrial Internet with extremely granular inspection, down to the machine transaction level. This provides the filtration, segmentation and isolation capabilities to secure large-scale OT networks.

Bayshore provides significant advantages over IT security solutions including:

- Off the shelf OT application and protocol domain knowledge
- Transformation of OT data for IT threat analytics
- Tailoring of policy to safety standards, government regulations and protection against insider threats
- Protection of manufacturing plants from cyber attack and operational errors
- Predictive maintenance
- Scalability to support global-scale OT infrastructure
- OT application layer policy enforcement
- Bayshore supports multiple deployment methodologies: on-premises, virtual appliance and hybrid cloud

Assurance of production uptime and reduced downtime

Predictive maintenance

Governance compliance and assurance

Scalability to support global OT infrastructure

Enhanced operational efficiency

Increased revenue, operational expense savings

Easier management – on-premises, virtual, cloud deployments

BAYSHORE
INDUSTRIAL CYBER PROTECTION

www.bayshorenetworks.com