BAYSHORE

USE CASE

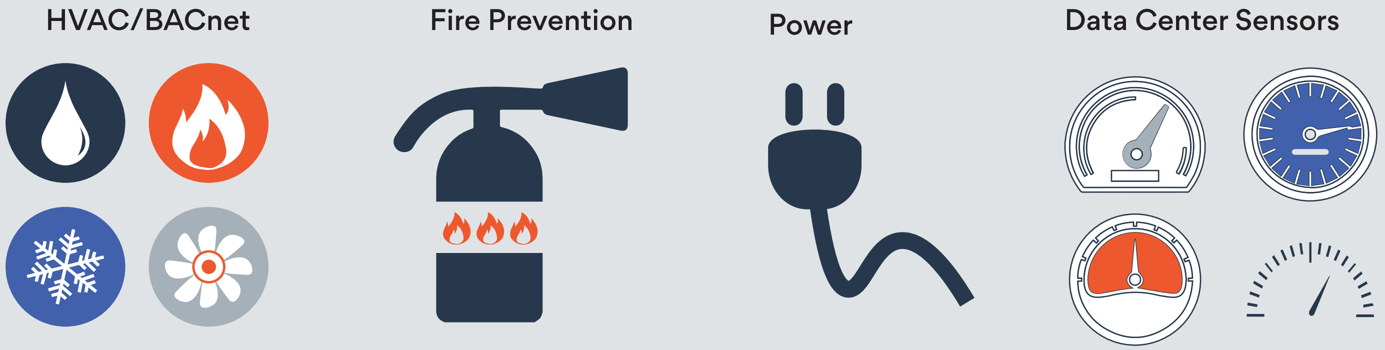
Data Centers

Today's Data Centers are vulnerable, exposed, and at high risk. Despite the increased threat of cyber attack around the world, most Data Centers and their associated Building Automation Systems have no Industrial Controls security policies in place. Vulnerabilities are everywhere. Security apertures can be opened by seemingly benign activities such as ping sweeps, use of sophisticated software applications, and, of course, by the use of default passwords.

Inside risks are exacerbated by convenience ports and weak control-system computers, which are often running back versions of Windows. Convenience ports enable the appearance of non-industrial traffic on the industrial system, which could introduce malware and provide additional attack apertures. Data Centers and Building Automation Systems present diverse environments that weren't intended to be connected to networks or the Internet. So standard IT security practices are ineffective.

Bayshore's software provides granular network controls and safety and security policies that are optimized for securing Data Centers. It collects Data Center telemetry (Building Automation, power, cooling, fire, etc.) and integrates it with Threat Management intel, automatically helping defend against known attack vectors.

TYPICAL DATA CENTER

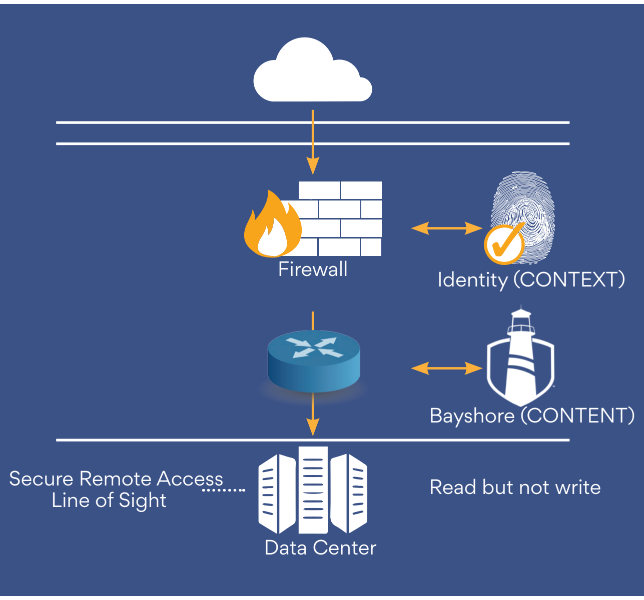


Security Requirements

- Protection of building automation systems and industrial controls
- Protection of communications from devices such as power equipment and field programmable gate arrays (FPGAs).
- Proactive cybersecurity, safety and operational policy
- Monitoring and analytics of silo'd data
- BACnet, EtherNet/IP, DNP3, IEC61850, GOOSE, and legacy serial protocols
- Predictive maintenance for IC
- Application segmentation and isolation

Bayshore's Data Center controls provide transformation of data into threat intelligence, threat prevention analytics, and performance analytics applications. They also enable:

- Secure remote access
- Diagnostics & troubleshooting
- Bi-directional security policies
- Safe and secure external visibility into Industrial Controls telemetry, such as Building Automation Systems



WHY FIREWALLS **DON'T SOLVE ALL**

- Because of data-level vulnerabilities.
- Must enforce safety rules such as Line of Sight.
- Monitor-only systems are NOT secure because they (or their attackers) may exceed the design functionality.

BAYSHORE POLICY POSES **CONDITIONAL QUESTIONS:**

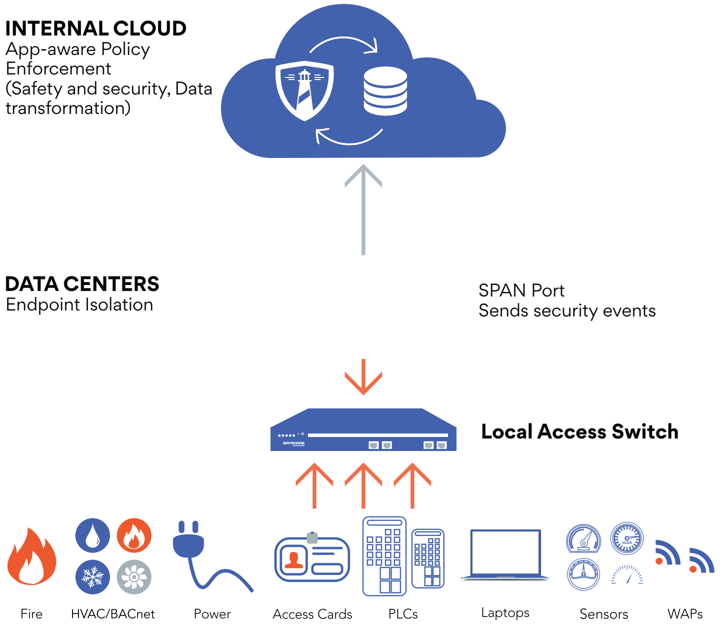
- "Are you in a safe and trusted zone?"
- "Are you asking my machines to do something that is unsafe or against policy"
- "Are you requesting telemetry that I shouldn't be sending to you?"

Outcomes

The Bayshore IT/OT Gateway ensures reduced risk with more secure operations, while maintaining stability of the Data Center and Building Automation environmentsv. Benefits of Bayshore typically include:

- Proactive prediction of Industrial Controls failures
- ROI associated with capital and maintenance costs (i.e. eliminate the need for redundant PLCs)
- Simplified, cost-efficient management of big data
- Aggregation of normalized telemetry data from multiple lakes into one big data platform.

SECURE TELEMETRY **AGGREGATION**



BAYSHORE

INDUSTRIAL CYBER PROTECTION

www.bayshorenetworks.com