AIRGAP

Securing the Manufacturing Industry

SOLUTION BRIEF

To remain competitive and gain operational advantages, today's modern manufacturers depend more heavily than ever before on automation, connectivity, and digital communications. The transformation to Industry 4.0 forces companies to combine next-generation technologies like IoT devices and Artificial Intelligence with existing/legacy OT solutions. This paradigm creates an environment that is difficult to protect and becomes a prime target for cyber threats like ransomware.

The creation of today's industrial control networks are a result of years or decades of devices and deployments. Cyber security was not a focus for most of these systems and is often overlooked or lacking completely.

As cyber threats and ransomware are increasing at an epidemic rate, the manufacturing sector is faced with many challenges protecting their IoT industrial networks. The most common issues are:

Visibility:
Industrial network device inventory is in constant flux. Manufacturers cannot secure communications between devices if all the devices are not identified and are constantly changing.

Control:
Given this complicated and ever-changing environment, controlling which devices can and should communicate makes enforcing even basic security practices a monumental task.

Productivity versus Security:
As IT and OT teams are forced to work together to implement, upgrade and secure these new industrial networks, balancing the need for security without impacting production is a difficult balance.