CASE STUDY

# Autonomous Zero Trust Policy Enforcement

This Fortune Global 500 electronics manufacturing services provider offers design, engineering and production to customers across a range of industries – from automotive to consumer products to advanced technology – around the world. The company is renowned for its efficient processes that meet and exceed service level agreements, consistently delivering value and results to its diverse customer base.

## The Challenge

Comprised of over 80 facilities worldwide, each of the company's manufacturing sites has its own individual network and security products, including a plethora of endpoint protection, VLANs, and ACLs. This infrastructure heterogeneity was difficult to manage and introduced an enormous potential attack surface.

## The Solution

To address these concerns, the CISO, head of the security operations center (SOC), and senior network engineer in charge of operational technology (OT) security developed a proof of concept to increase cohesion from site to site, minimize the attack surface, simplify processes, and increase security on the production floors. They decided that Airgap's zero-trust approach to security would be the most effective strategy, allowing assets to be isolated within the same network or VLAN without requiring a personal firewall in front of each device.

## The Result

The team deployed Airgap's Zero Trust Isolation™ platform and saw immediate results. "Endpoint protection was causing a lot of issues on our production machines," said the Sr. Network Engineer of OT Security. "With Airgap we were able to remove the overhead of endpoint malware security products and get better protection and visibility across the board."

Airgap's agentless solution is used to completely isolate devices and set specific exceptions, providing the company with an increase in stability and performance across all manufacturing floors. The senior engineer continued, "With Airgap we have much better isolation, so the potential of a malware or ransomware outbreak is not really an issue – the attack surface has been reduced by a tremendous amount."

Additionally, the team leveraged Airgap's agent-less microsegmentation capabilities. "Collaboration and production security are the top priorities for my team," said the senior engineer, "and complicated segmentation can quickly overwhelm the resources we have available." Airgap's agentless segmentation allowed the team painlessly ringfence every device and application, preventing lateral threat movement and stopping the potential of malware and ransomware propagation.

> "With **Airgap** we have much better isolation, so the potential of a malware or ransomware outbreak is not really an issue – the attack surface has been **reduced by a tremendous amount.**"

## About Airgap Networks

Airgap delivers the industry's first Zero Trust agentless segmentation solution that works at the intersection of IT and OT to ensure your organization stays secure from external and internal threats. Based on Zero Trust principles, Airgap prevents lateral threat movement, only allows authorized and authenticated access to high value assets, and ensures rapid incident response via its patented Ransomware Kill Switch™ solution. Airgap is easy to deploy with no forklift upgrades or infrastructure changes. Customers often start seeing the results within a few minutes of deployment.

AIRGAP™

**airgap.io**