AIRGAP

# Protecting Critical Assets Against Ransomware Attacks

FACTORIES. DATA CENTER. CLOUD.

## Airgap - Manufacturing (Purdue Model)

| | | | | |
|---|---|---|---|---|
| Level 5 | Email | Saas | PaaS | NGFW |
| Level 4 | ERP | CRM | SCM | NGFW / AIRGAP |
| DMZ | Jump Server | Patch Mgmt. | Jump Server | AIRGAP |
| Level 3 | Historian | IIOT Platform | Workstation | AIRGAP |
| Level 2 | HMI | SCADA Server | HMI | AIRGAP |
| Level 1 | PLC | SCADA | PLC | |
| Level 0 | Sensor | Actuators | Sensor | Actuators |

**Perimeter Firewall:** Protect from the outside-IN threats and secure connectivity b/w sites

**Interzone Firewall:** Visualize and control the communication between different zones

**Secure Access:** Reduce attack surface and enable SSO/MFA authenticated access

**Lateral Threat Movement Prevention:** Provides visibility and control to protect against intra-VLAN threat movementauthenticated access

**Line Isolation:** Segregates different endpoints in production lines. Provide strict controlled access to the Layer 3 endpoints

## Why Only Airgap? Technology Fit For Factories

### Agentless Network Segmentation

Only solution that prevents **intra VLAN lateral threat movement**. All threats are confined to a single endpoint.

### Agentless Secure Access

Only solution that ensures SSO/MFA based **secure access to high value assets** on factory floors. Hides vulnerable protocols.

**Protect high value assets against lateral threat movement**

## Airgap & NG Firewall: Roles and Responsibilities

| Role / Responsibilities | Airgap Isolation | Next-Generation Firewall |
|---|---|---|
| **Visibility** | Visualize **intra** VLAN communications | Visualize **inter** VLAN communications |
| **Profiling & Auto Grouping** | Autonomous grouping based on **device type, OS, manufacturer** etc. | Dynamic grouping based on device behavior (require CDL and IOT licenses) |
| **Segmentation** | Granular/per-device segmentation (**"Segment of One"**). Ringfence every devices from each other | Segmentation based on VLANs, Subnets, and Zones |
| **Policy Enforcement** | Enforce **intra** VLAN policies using autonomous devices groups. Stop lateral threat movement. | Enforce **inter** VLAN polices using subnets, interface, object groups and zones. |
| **Threat Protection** | Detect and block lateral VLAN threats from **one device to another** (insider threats) | Detect and block **outside-IN threats** (emerging from internet) |
| **Rapid Response** | Automated enforcement using **Ransomware Kill Switch** | N/A |
| **Secure Asset Access** | **Just-in-time** access with SSO / MFA for high value equipment. Hides vulnerable ports / protocols | N/A |

## Airgap: Proof of Value

**Ringfence IP endpoints and provide visibility & control all lateral traffic. Reduce attack surface on high-value assets**

1. Ringfence every devices in a VLAN and create a logical grouping based on type / production lines
2. Visualize all "intra" VLAN traffic
3. Policy control for "intra" VLAN traffic
4. Protection for static or DHCP based devices
5. Zero false detection of offending devices
6. 1-click quarantine (block all network access)
7. Enforcement of rapid response policies
8. Enable JIT/JET access using SSO/MFA
9. Hide vulnerable ports protocols from advisories
10. No VLAN, no subnet, no zone, no network redesign




## Airgap Isolation: Agentless Segmentation Platform

**Time to value in hours, without requiring network redesign**

**Best-in Class Agentless Zero Trust Segmentation**

**Ringfence every IP endpoint** in its own network

Visualize and **control intra-segment** or intra VLAN traffic

**Lateral Threat Movement Prevention**

**Zero false positive** lateral threat detection and prevention

**Ransomware Kill-Switch** for rapid incidence response

**Ease of Use – Software Solution**

**Agentless** & standards based – supports all endpoints

**Seamless migration** – one VLAN or one endpoint at a time

## About Airgap

Airgap provides an agentless Anti-Ransomware platform to stop the spread of malware in the enterprise network. Our industry's first Ransomware Kill Switch™ locks down your most critical network assets at the first indication of compromise with complete control and policy enforcement over the device-to-device and device-to-application communication.

**airgap.io**

AIRGAP