CASE STUDY

Prominent Digital Printer Launches Agentless Segmentation in Response to Ransomware Attack

Airgap's patented network security solutions are custom designed to minimize the enterprise attack surface and protect high-value assets in manufacturing, healthcare, retail, and critical infrastructure verticals where a compromise of the core operating system can disrupt mission-critical processes. Airgap Security Platform is the easiest to implement and manage and it is currently deployed across many large multinational customers.

This case study reveals how Airgap employed agentless segmentation and zero-trust protocols to protect a client from ransomware attacks.

The Client

A major digital printing operation specializing in short and medium runs of custom and RFID labels, shrink sleeves, flexible packaging, and wide-format products in low industry quantities came to Value Creed for help after its manufacturing lines fell victim to ransomware in November 2020.

Challenges

At the time of the ransomware attack, the printer operated via a flat matrix involving all users across five manufacturing sites in the Midwest and Desert Southwest. The company linked everything from telephone systems to mission-critical machinery within the same network. And it had not taken any steps to separate its IT and OT networks.

The Airgap Solution

To prevent a repeat attack, Airgap in early 2021 implemented its Zero-Trust Isolation Gateway as a pilot program in one of the company's manufacturing locations. Airgap Zero Trust Isolation supports all endpoints and performs profiling and autonomous grouping based on the device type and network.

Employing agentless segmentation helps the print manufacturer monitor the network traffic along all OT/ IT devices. Airgap has ringfenced every IP endpoint, providing a peerless threat detection and prevention mechanism. When the isolation gateway verifies that an attacker is attempting to penetrate the company's OT network, it triggers Ransomware Kill Switch, Airgap's specially-built response platform that surgically stops ransomware propagation without operational disruption.

Airgap and the client agreed on the need for sub-second recovery time objective (RTO) with full zero trust assurance. While Airgap supports installation on bare metal, container images, physical appliances. or virtual instances, the optimal configuration for this client called for Airgap Zero Trust Isolation Gateways to be deployed on the company's Hyper-V hypervisor and Microsoft virtualization environment. This allowed for full high availability (HA) and Active – Hot Standby configuration enabling instant failover should downtime occur

The solution employs two Airgap Zero Trust Isolation Gateways deployed on one site.

The Results

This architecture ensures the client receives the protection it needs to prevent, detect, and eliminate future ransomware attacks:

1. **Dedicated monitoring of traffic on each device at the manufacturing site.**
2. **User classification performed based on type and production line.**
3. **Visualization and documentation of all "intra" VLAN traffic.**
4. **Full user customization of policy controls as informed by this "intra" VLAN traffic.**
5. **Manual quarantine of any suspicious endpoints to block all network access to and from the infected device**
6. **Airgap-provided Zero-Trust incident response in case of an attack that mobilizes Ransomware Kill Switch.**
7. **User-enabled SSO/ MFA-based access for factory equipment to hide vulnerable ports and protocols from advisories.**

The success of Airgap's pilot program has led the client to plan the expansion of the agentless Zero-Trust platform into its remaining four sites in 2022

About Airgap Networks

Security experts know that network segmentation is the best defense against evolving cyber threats. However, available segmentation solutions either require agents to be installed everywhere or necessitate networking hardware upgrades with proprietary implementations. Airgap is the only vendor that offers agentless network segmentation and autonomous policy controls through a patented and innovative approach that enables isolation at every layer and down to every device. All this means malware is immediately blocked from traversing the network, even within the same VLAN or same subnet - unique protection not offered by any other solution.

Additionally, a typical organization takes hours or days to detect and respond to ransomware attacks and often resorts to a draconian approach of shutting down the entire network during a cyber event resulting in operational impact. Therefore, Airgap built a specialized ransomware kill switch that surgically stops ransomware propagation without operational impact.

Finally, enterprises often enable direct access to high-value assets over vulnerable protocols such as Windows RDP. Airgap's identity-based access control provides strong Zero-Trust safeguards as a layer of protection to secure enterprise assets against cyber threats.

AIRGAP™

airgap.io