AIRGAP

Zero Trust Isolation

SOLUTION BRIEF

Solution Overview

Ransomware and malware continue to wreak havoc across all industries. This is due to an exploitable networking vulnerability that stems from the perimeter centric security model: devices on a shared VLAN have a complete view and communication path to all other devices. Furthermore, static security policies implemented over next generation firewalls (NGFW) are ineffective in restricting network level access to business applications.

These vulnerabilities lead to IT teams unwittingly building expressways for ransomware, which are effectively used by bad actors to expand the attack.

Zero Trust Isolation addresses these critical security challenges, offering an optimal defense against cyber threat propagation. Airgap works under the assumption that every device is breached or will soon be breached. This zero-trust enforcement model contains the spread of ransomware and malware to a single device.

Infected devices are ring-fenced so that threats cannot be propagated beyond isolated devices. Without Zero Trust Isolation, the breached laptop in the middle of *Figure 1* would infect the other devices on the shared VLAN.

Figure 1: Lateral Propagation is Stopped by ***Zero Trust Isolation***

CHALLENGE

A global army of bad actors is constantly using new attack vectors to spread malware and ransomware. Once a sophisticated hacker breaks a perimeter, it's quite easy to infect many devices through lateral propagation on shared VLANs.

The traditional perimeter model for segmentation and isolation is ineffective because devices on a shared VLAN have a complete view and communication path to all other devices. An alternative is to implement a Zero-Trust architecture, but this is generally complex and expensive to do, requiring agents and infrastructure changes. A simpler solution is needed.

SOLUTION

Airgap's Zero Trust Isolation prevents lateral threat propagation by isolating devices from each other. The solution protects your organization even if:

- Some of your endpoints are breached
- You have vulnerable and unpatched applications
- You are using legacy and insecure protocols

Airgap's Zero Trust Isolation is easy and fast to deploy, and requires no agents, APIs, or design changes. It provides a rapid, seamless migration to a zero-trust architecture. And Airgap's Zero Trust Isolation can be rolled out incrementally—one device or one VLAN at a time.

KEY BENEFITS

- Agentless solution that can be deployed in minutes
- Protects managed and unmanaged devices
- Allows phased migration with no APIs or design changes
- Offers total visibility into all lateral communication
- Restricts the "blast radius" of ransomware attacks
- Protects corporate applications and enterprise "crown jewels"

Airgap's Zero Trust Isolation prevents the attack from propagating to other devices. This patent-pending technology inverts the traditional "shared trust" model, uniquely isolating devices from each other. Only authorized traffic is permitted between devices.

Once deployed, Zero Trust Isolation starts learning and providing visibility for all device-to-device communications. Using multiple profiling techniques, the solution accurately identifies the device type, grouping each device based on its characteristics.

Enterprises can deploy the solution in brownfield or greenfield networks without the need for forklift upgrades, end-point agents, changes to applications, or the need to update any existing security tools. The standards-based implementation also works with a variety of devices including managed or unmanaged devices.

Zero Trust Isolation continuously monitors all device-to-device lateral traffic within the shared VLAN and offers complete visibility to the IT organization *(Figure 2)*.

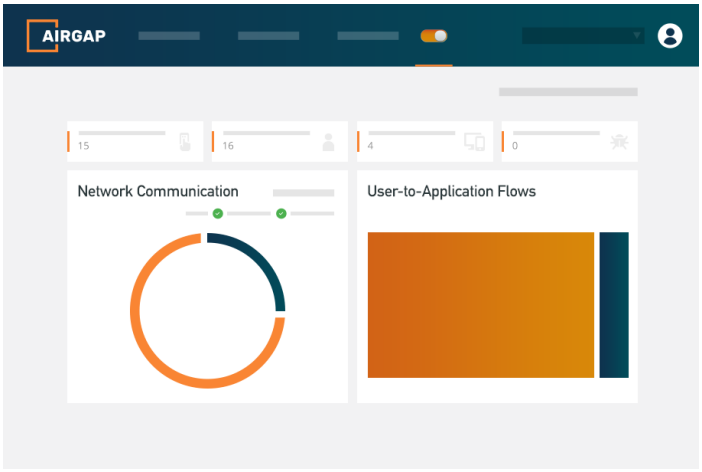

Figure 2: Interdevice Traffic Chart

Airgap also prevents malware propagation to private applications by restricting network level access and enforcing Single Sign-on/ Multi-Factor Authentication (SSO/MFA) challenges to verify the access request intent.

Key Features

Table 1 highlights the key features of the solution.

Table 1: Key Features

FEATURE	DESCRIPTION
Safeguard against legacy protocol vulnerabilities	Auto-profile legacy protocols and permit only authorized traffic
Lateral traffic visibility	Provides visibility for lateral traffic flows, including all communications (authorized or unauthorized) between all devices in a shared VLAN
Proactive protection	Granular, controlled, and automated policy enforcement for unauthorized traffic. Confines ransomware/malware to a single device
Protects private applications from untrusted users and devices	Reduces the attack surface on enterprise private applications by eliminating network level access
Enables Ransomware Kill Switch	This emergency network shut-off minimizes ransomware propagation and business disruption
Transparent deployment	Zero trust enforcement without the need for end-point agents or changes to applications; integrates with existing infrastructure
Flexible phased migration	Enterprise may choose to migrate a few devices or individual subnets/VLANs at a time to Airgap

Enablement of Ransomware Kill Switch

Airgap's Ransomware Kill Switch is designed to mitigate ransomware impact on a network. This patent-pending mechanism is the industry's only solution that instantly locks down lateral communications and denies access to vulnerable critical assets. There is minimal or no disruption to users and businesses.

Autonomous Policy Control

Zero Trust Isolation includes a policy framework built using device grouping. Groups are created based on device type and attributes. Stateful firewall policies are defined for traffic from one group to many groups. Airgap's autonomous grouping is built with rich device profiling capabilities so that security policies are automatically updated as new devices are added to the network.

Management and Orchestration

A centralized cloud-hosted management control provides configuration and management access to the gateway. Capabilities include visibility of all lateral communications, application access requests, and full compliance logging with a highly redundant, scalable system supporting full multitenancy and Role-Based Access Control (RBAC).

About Airgap

Airgap addresses the most fundamental security challenges faced by IT organizations. It's Zero Trust Isolation solutions are trusted by leading managed service providers and enterprises. Based out of Silicon Valley, California, the venture backed company is founded by highly experienced cybersecurity experts.

To learn more or to schedule a demo, please visit us at https://airgap.io or contact us at info@airgap.io.