SOLUTION BRIEF

Anywhere Agentless Zero Trust Segmentation

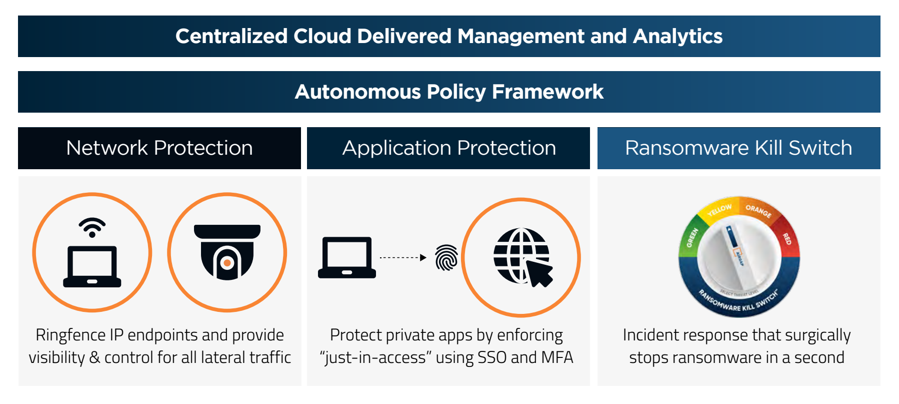
Workload security at any cloud scale for any identity

Agentless, Simplified Zero Trust Segmentation

Many organizations halted their network segmentation projects with legacy segmentation products and firewalls due to the complexity, cost and intensive IT network virtualization expertise needed.

Airgap Agentless Zero Trust Isolation platform inherently simplifies network segmentation with granular context-based policy enforcement to secure your attack surfaces. From enterprise entities to remote sites, the single cloud-delivered SaaS platform with distributed and elastic isolation gateways secures your workloads across the Clouds.

Airgap's agentless and patented zero trust in-line approach eliminates lateral cyberattacks and ransomware movement by isolating the workload dependency from applications, identity and network. As the first hop of any packet, Airgap provides the modern zero trust micro-segmentation solution that delivers intent-based behavior observability, dramatically automates policy grouping & enforcement, and surgically eliminates ransomware incident responses with actionable Ransomware Kill Switch™ in real time.



Centralized Cloud Delivered Management and Analytics

Autonomous Policy Framework

Network Protection | Application Protection | Ransomware Kill Switch

Ringfence IP endpoints and provide visibility & control for all lateral traffic

Protect private apps by enforcing "just-in-access" using SSO and MFA

Incident response that surgically stops ransomware in a second

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.

Zero Agent. Zero Trust.

Instead of worrying about patching agents and endless future maintenance costs. Agentless is the only way for your zero trust segmentation solution.

Airgap's Agentless 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. Airgap's 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.

Airgap's Agentless Anywhere Segmentation approach is completely agentless and built to safeguard across your applications, clouds, data centers, and workloads at scale with modern cloud-native service integration for extremely high throughput and low latency performance.

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"

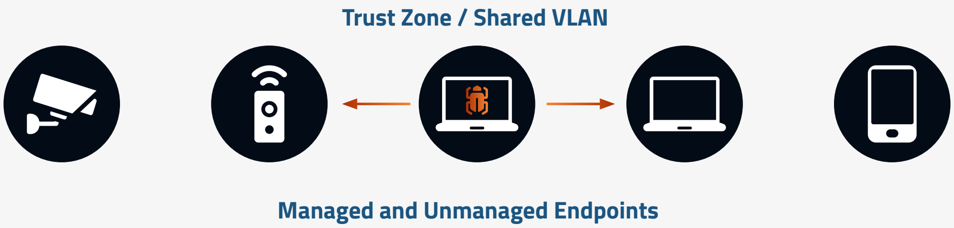


Figure 1: Lateral Propagation is Stopped by Zero Trust Isolation

Real-Time Agentless Discovery and Observability

Airgap's patented approach to Zero Trust Segmentation starts learning and providing visibility for all device-to-device and device-to-application workload communications using multiple profiling techniques for immediate benefits of giving you a holistic view of all IT/OT/IOT workload communications across heterogeneous workloads anywhere.

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.

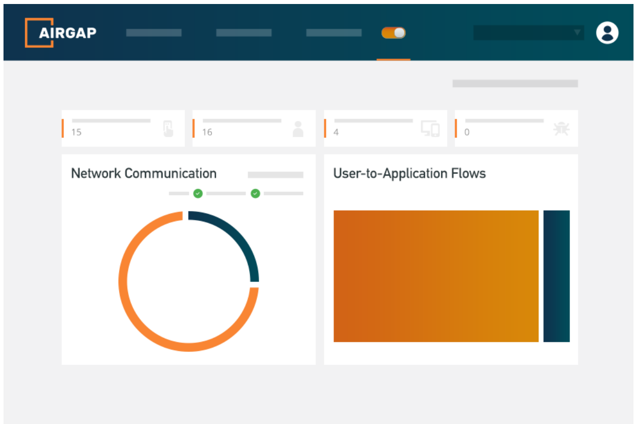


Figure 2: Interdevice Traffic Chart

Secure Asset Access

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.

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	Enables rapid incident response with the emergency shut-off and surgically eliminates ransomware propagation
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
Agentless Segmentation	Real-time network control or visibility for managed and unmanaged devices. Eliminate error-prone patch deployment and management.
Full programmability and SIEM/ SOAR platform integration	Support cloud-first initiatives and digital transformation with fully programmable APIs. Built-in integration with leading SIEM/SOAR platform for advanced traffic and access log analytics
Location-agnostic segmentation	Support Zero Trust Anywhere Agentless Segegmentation on premises and Public Cloud

Autonomous Policy Control Across Clouds

Airgap Zero Trust Isolation platform includes a unified 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. It dramatically eliminates the complexity and painful design in policy creation and fine-grained segmentation security controls.

Security policies are **automatically updated** as new devices are added to the network

Cloud-Delivered Management and Orchestration

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

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