Airgap Zero Trust Isolation Platform

DATA SHEET

THE CHALLENGE

Despite continued spending of hundreds of billions of dollars on security solutions, ransomware and malware continue to wreak havoc across all industries. A single infected device on a network can propagate malware and bring down an entire network in seconds. Even worse, the ransomware can stay in stealth mode and slowly penetrate the organizations critical assets e.g. file-share, applications, accessing and stealing customer or employee sensitive data.

A global army of ‘Bad actors’ are constantly searching for new threat vectors to attack networks. As soon as a perimeter is breached, the attackers can freely traverse shared VLANs and search for weaknesses such as unpatched devices and servers.

> The traditional segmentation and isolation designs using shared Virtual Local Area Network (VLANs) and firewalls have two fundamental flaws
>
> - In the same VLAN all devices can see and communicate with each other
> - Static and outdated policies based on VLANs, IP addresses, or zones allowing network level access to applications

Added together, shared VLANs and static policies have created a data superhighway, that after careful analysis by Airgap, is primarily used by ‘bad actors’ to propagate malware/ransomware within networks.

Airgap Networks Zero Trust Isolation Platform solution addresses these identified flaws in legacy network blueprints by isolating devices from each other, which in turn halts lateral threat propagation. Airgap also protects private applications by eliminating network level access.

AIRGAP ZERO TRUST ISOLATION PLATFORM OVERVIEW

Airgap Zero Trust Platform addresses some of these critical security challenges, offering the best defense against cyber threat propagation for IT organizations.

> Airgap works under the assumption that every device is breached OR will soon be breached. Which means that a zero-trust architecture is the best way to minimize the extent of any attack.

Airgap introduces zero-trust enforcement on the shared network (e.g., VLANs) and application access, which contains the spread of ransomware and malware to a single device.

Once deployed, Airgap Zero Trust Isolation (ZTI) Platform starts learning and providing visibility for all device-to-device communications. Our patent pending technology then inverts the traditional shared trust model concept, uniquely isolating devices from each other, and permits only risk-free authorized traffic.

Airgap also prevents ransomware/malware propagation to private applications by restricting network level access and enforcing SSO/MFA challenges to verify the access request intent.

Enterprises can deploy the Airgap ZTI platform in brownfield or greenfield networks without the need for forklift upgrades, end-point agents, changes to applications, or the need to remove any existing security tools. Its standard-based implementation works with any device managed or unmanaged, and IoTs alike, and will be transparent to the end-user experience or behavior.

KEY FEATURES

Lateral traffic visibility:
Providing visibility for all traffic flows, including authorized and unauthorized communications, between all devices in a shared VLAN.

Proactive protection:
Granular, controlled and automated policy enforcement for unauthorized traffic. Confining threats such as ransomware and malware to a single device.

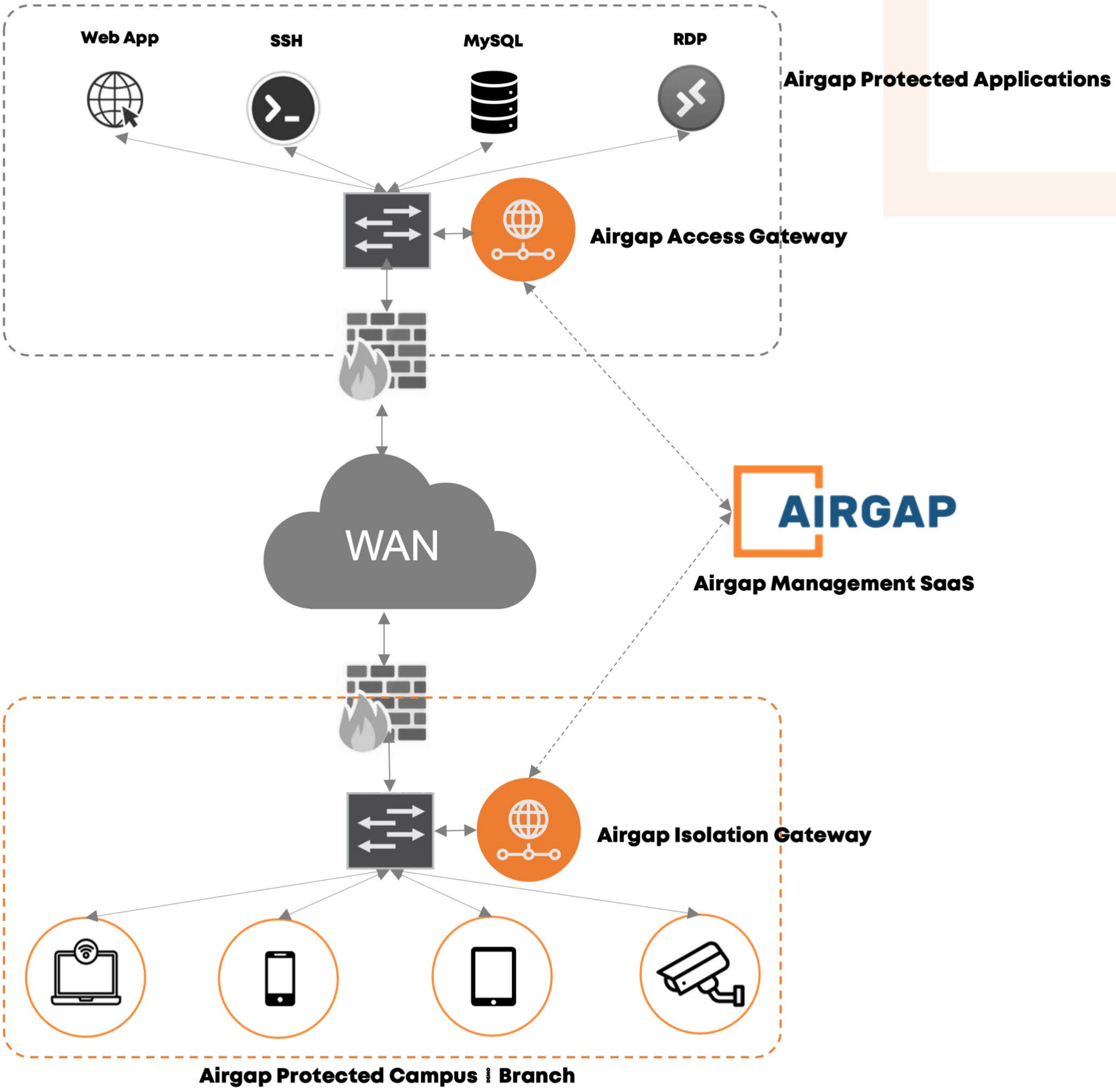
Lock-down network with “1-Click” during a ransomware emergency:
An emergency network shut-off switch (Airgap Ransomware Kill Switch) minimizes ransomware propagation and business disruption.

Protecting private applications from untrusted users and devices:
Reduce the attack surface on enterprise private applications by eliminating network level access. While adding additional security by requiring SSO and MFA for any user, any device, from any location.

Transparent deployment:
Zero trust enforcement without the need for end-point agents or changes to applications. Airgap’s solutions can easily be integrated with existing infrastructure

Frictionless staged migration:
Airgap solutions are a SaaS based offering with a cloud delivered management system. Allowing easy migration to a secure Airgap network solution.

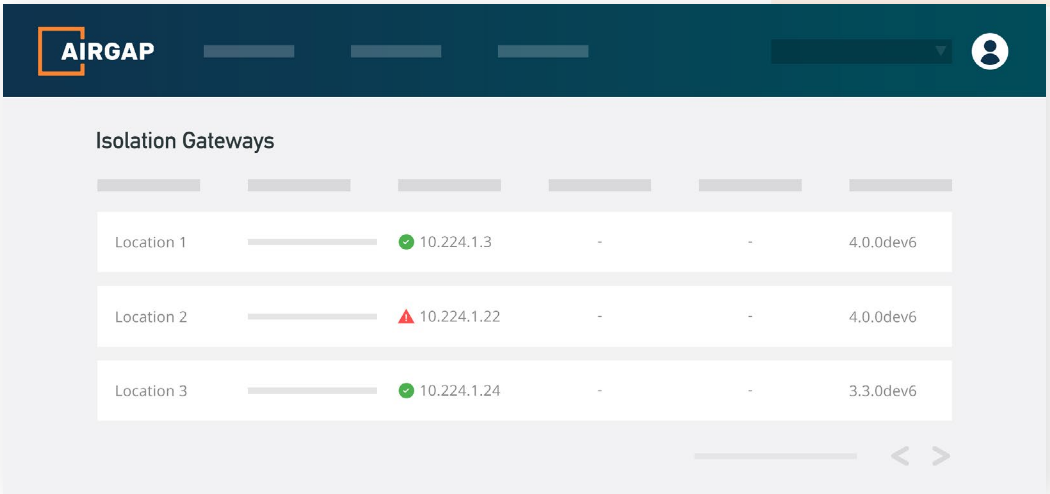
ARCHITECTURE



ARCHITECTURE

AIRGAP ISOLATION GATEWAY

Using a virtual machine connected to the same VLAN or network (via a Layer2 switch) as the devices requiring protection. Once installed the Airgap Isolation Gateway begins isolating devices from each other and permitting authorized device-to-device lateral communications only. The gateway will also be responsible for device profiling, detection of abnormal devices, and uncovering threats that may hide in the shared network. For redundancy and high availability, multi gateways can be deployed in an N+1 configuration.

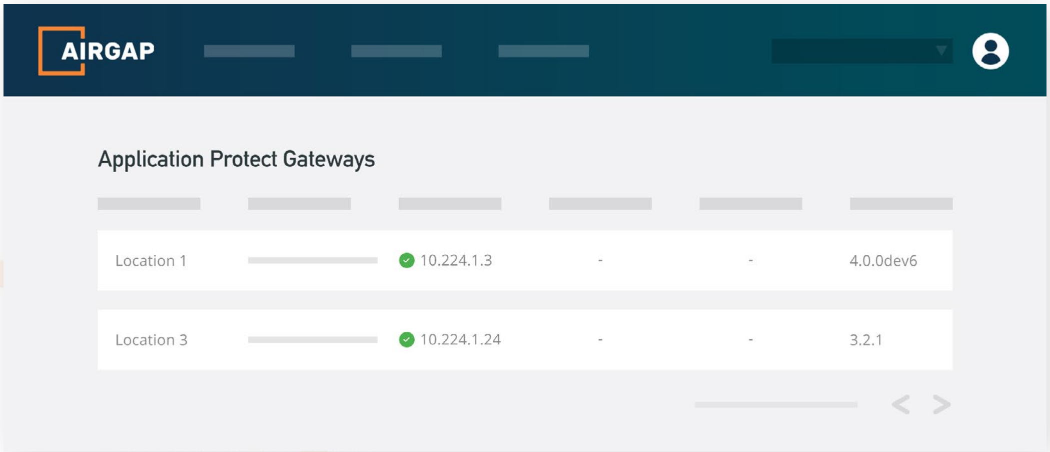


Isolation Gateways

Location 1		✓ 10.224.1.3	-	-	4.0.0dev6
Location 2		⚠ 10.224.1.22	-	-	4.0.0dev6
Location 3		✓ 10.224.1.24	-	-	3.3.0dev6

AIRGAP ACCESS GATEWAY

Using a virtual machine deployed in the DMZ zone or on the same network as the organization's private applications. The Airgap Access Gateway will act as a multi-protocol proxy for the enterprise authorized Single Sign ON (SSO). All requests to private applications, including Web, SSH, RDP, etc. the gateway will be the explicit proxy, hiding and protecting private applications from network layer exploits.



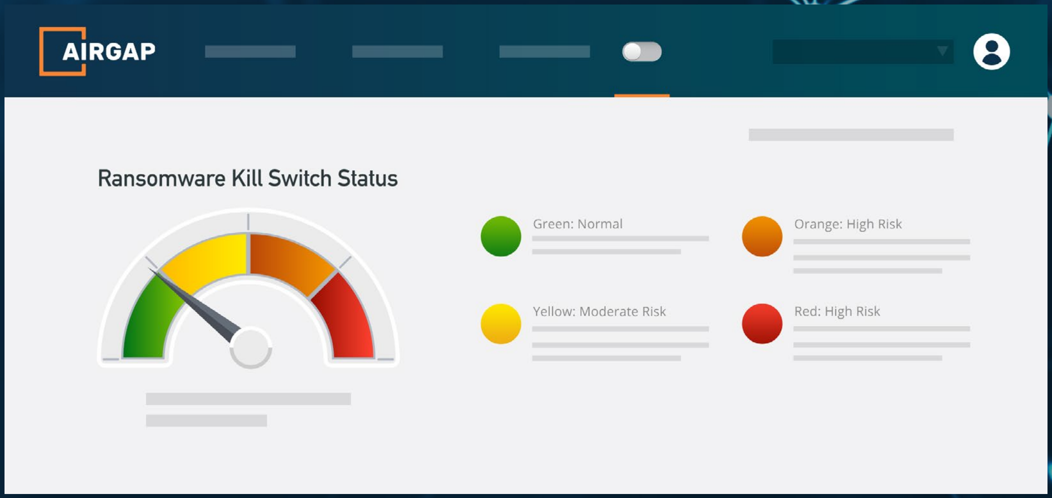
Application Protect Gateways

Location 1		✓ 10.224.1.3	-	-	4.0.0dev6
Location 3		✓ 10.224.1.24	-	-	3.2.1

ARCHITECTURE

AIRGAP MANAGEMENT AND ORCHESTRATION

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



KEY FEATURES

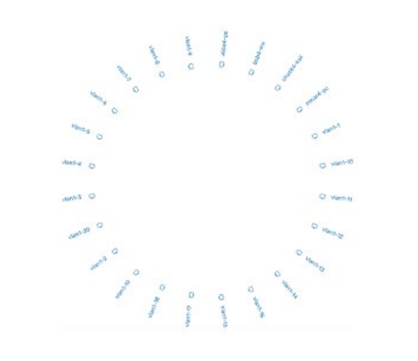
AIRGAP VISIBILITY

Airgap provides a visual representation of every device on the network. Using multiple profiling techniques. Airgap ZTI accurately identifies the device type, grouping each device based on its characteristics.

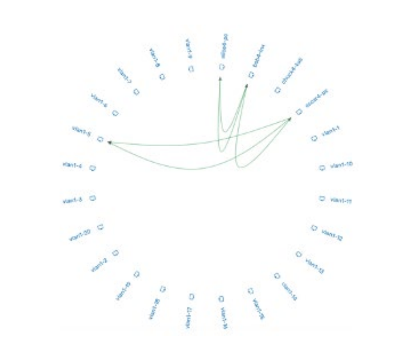
Airgap ZTI continuously monitors all device-to-device lateral traffic within the shared VLAN and displays this information in an intuitive chart. The device-to-device communication chart provides extensive color coding, filtering, and application identification for all lateral traffic. NOC/SOC teams can now learn about threats and unknown communications in the shared network (e.g., Intra VLAN traffic), previously not possible with existing networking and security tools.

KEY FEATURES

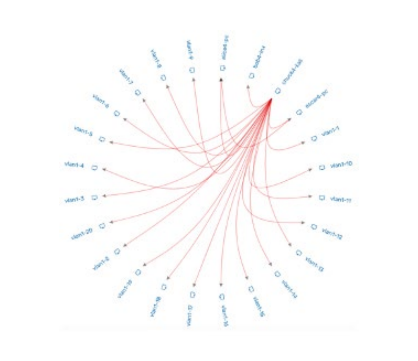
SNAPSHOTS FROM AIRGAP MANAGEMENT CONSOLE



Network devices



Permitted Traffic



Denied Traffic

AIRGAP RANSOMWARE KILL SWITCH

Airgap Network's "Ransomware Kill Switch (RKS)" is designed to mitigate ransomware's impact on a network. The patent-pending idea 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 the users and businesses.

In a ransomware emergency, the RKS enforces a lock-down based on degrees of severity. The Platform provides easy color-coded options (e.g., Green, Yellow, Orange, and Red) and a policy framework to customize the severity.

POLICY CONTROL BASED ON MALICIOUS ATTACK SEVERITY LEVEL

● SYSTEMS NORMAL

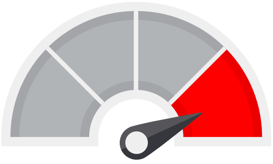
Protect the network and enforce system policies

● MODERATE RISK

Protect the network and enforce Yellow policies

● HIGH RISK

Protect the network and enforce Orange policies



● CRITICAL RISK

Protect the network and enforce Red policies

KEY FEATURES

AIRGAP AUTONOMOUS POLICY CONTROL

In modern enterprises, devices and their IPs are continually changing. The Airgap policy framework is built using device grouping to support this dynamism. The groups are created based on the device type and their attributes, e.g. manufacturers, operating systems, and service offerings. The stateful firewall policies are defined for traffic from one group to many groups.

Airgap Autonomous capabilities take this concept a step further by continually updating the groups. Enforcing business policies as the devices enter and leave the network. E.g., When a new Windows 10 laptop connects to the network, it will be automatically added to the Windows OS group which has pre-defined policies for Windows OS systems.

AIRGAP SECURE APPLICATION ACCESS

Airgap's Zero Trust Isolation (ZTI) platform implements a multi-protocol proxy, acting as a bullet-proof shield, that protects business-critical private applications from untrusted users and devices.

Unlike traditional firewalls, VLANs, Subnets, Zones, or VPN based access, Airgap employs a Single Sign-On (SSO) and Multi-Factor Authentication (MFA) providing strict identity-based access. Since Airgap is acting as an explicit proxy, the end-users and devices will never be permitted to have network-level access to the applications.

Along with Web-based applications, Airgap also supports SSO/MFA based session layer access to non-web-based applications like SSH, RDP, Databases, etc. This ensures the vulnerable legacy protocols like RDP, Telnet, etc. are never exposed to any user.

Airgap Secure Application Access works with any browsers, native SSH, or RDP clients without requiring any tunnels or data-path agents.

About Airgap Networks Inc.

Airgap's Zero Trust Isolation Platform offers the best defense against cyber-threat propagation. Airgap's patent pending solution works for any user and any device accessing business assets from any location and it can be installed in a few minutes without any forklift upgrades. Trusted by leading managed service providers & enterprises, Airgap addresses some of the fundamental security challenges faced by the IT organizations. To learn more or to schedule a demo, please feel free to visit us at https://airgap.io or contact us at info@airgap.io

AIRGAP